Manual de Operações

Gateway AG 30

Julho de 2014, 200.0520.00-0 Rev. 011

Copyright© Digistar, São Leopoldo - RS, Brasil.

Todos os direitos reservados.

A Digistar se reserva o direito de alterar as especificações contidas neste documento sem notificação prévia. Nenhuma parte deste documento pode ser copiada ou reproduzida em qualquer forma sem o consentimento por escrito da Digistar.

Sumário

1. Conhecendo o seu Gateway 4
1.1. Conteúdo da Embalagem 4
1.2. Características Técnicas 4
1.3. Descrição do Hardware 6
1.3.1. Painel traseiro do Gateway Digistar 6
1.3.2. Painel frontal do Gateway Digistar 7
2. Acessando o Configurador Web Digistar 8
2.1. Login 9
3. Configurações de Sistema 13
3.1. Rede 13
3.1.1. Configurações de Rede e DHCP 13
3.1.2. Configurações de Roteamento Estático 15
3.1.3. Configurações de Multicast 17
3.1.4. Configuração de Certificados 18
3.1.5. Configurações do DNS Dinâmico 19
3.1.6. Configuração de VLAN 19
3.1.7. Configurações de NAPT 20
3.2. Firewall 21
3.2.1. Configurações Gerais 22
3.2.2. Filtros DoS 23
3.2.3. Filtros de Usuário 25
3.2.4. Filtros de Conteúdo 26
3.3. VoIP 27
3.3.1. Configuração do SIP 28
3.3.1.1. Habilitar SIP (Configurações Gerais) 28
3.3.1.2. Habilitar Servidores SIP 29
3.3.2. Configurações SIP Integrado 31
3.3.2.1. Configurar Contas SIP 32
3.3.2.2. Configuração de RTP 33
3.3.3. Configuração do NATT 33
3.3.4. Configurações de QoS 34
3.4. VPN 37
3.4.1. Configurações do PPTP 37
3.4.2. Configurações do L2TP 45
3.4.3. Configurações do IPSEC 53
3.5. Serviços 55
3.5.1. Configurações de Data e Hora 55
3.5.2. Configurações de SNMP/Syslog e Radius 57
3.5.3. Troca do MAC 58
3.5.4. Servidor FTP 58
3.6. TDM 61
3.6.1. Tronco Digital 61
3.6.2. Ganhos 64
3.6.3. Grupos 64
3.6.4. Redirecionamento 66
3.6.4.1. Adicionar Regra 66
3.6.4.2. Expressões de Associação 68
3.6.4.3. Expressões de Substituição 68
3.6.4.4. Ordem de execução das regras 69
3.6.5. Casos de uso 69
3.6.5.1. Caso 1 69
3.6.5.2. Caso 2 71
3.6.6. Status 72
4. Manutenção 73
4.1. Firmware 73
4.1.1. Versões 73
4.1.2. Upgrade de Firmware 73
4.2. Configuração 74
4.2.1. Download 74
4.2.2. Upload 75
4.3. Misc 75
4.3.1. Mensagens Binárias 75
4.3.2. Reset Geral 75

5. Anexo I - Status enviado do SIP para o ISDN no encerramento de ligações. 76

Prezado Cliente:

Leia atentamente este Manual de Operações para entender o funcionamento de seu Gateway Digistar, além de providenciar o local adequado para sua instalação.

Caso persista alguma dúvida, entre em contato com o seu instalador.

Considere-se bem-vindo à Digistar Telecomunicações.

É motivo de grande satisfação para nossa empresa tê-lo como cliente.

Termo de Garantia:

Para utilizar os serviços de garantia de seu Gateway Digistar, você precisará apresentar cópia da Nota Fiscal de Compra do produto, com data de emissão legível e enviar para o Centro de Reparos da Digistar (CRD). As despesas com frete serão por conta do cliente.

Suporte Técnico:

Ao contatar o Suporte Técnico da Digistar, tenha as seguintes informações disponíveis:
- Modelo do produto;
- Informações sobre a garantia - dados da Nota Fiscal de Compra;
- Uma breve descrição do problema;
- Nome da empresa que instalou o produto.

Método	Descrição
E-mail Suporte	suporte@digistar.com.br
Telefone	(51) 3579-2200
WEB Site	www.digistar.com.br

1. Conhecendo o seu Gateway

O AG 30 é um gateway que converte tecnologias:

- Converte a tecnologia IP em digital, permitindo que uma rede IP (VoIP) faça a interface de voz, via E1, com a rede PSTN, agregando pontos de presença em diversas localidades e com o custo de uma chamada local.

- Converte a tecnologia digital de um PABX TDM (E1) em IP, permitindo o uso da tecnologia VoIP, sem alterar o PABX existente.

Observação: Ao longo deste manual o AG 30 será denominado de "Gateway Digistar."

1.1. Conteúdo da Embalagem

- ✓ 1 Gateway Digistar
- ✓ 1 Manual de instalação
- ✓ 1 CD de Documentação do Produto
- ✓ Fonte de alimentação

1.2. Características Técnicas

Rede: • Roteamento Estático: host ou rede • DNS Dinâmico • Certificados digitais: Garantia de autenticidade e segurança, cada Gateway Digistar terá um FQDN ou IP diferente. • VLAN (802.1q)	**Interface WAN:** • Modo Brigde • Cliente DHCP • IP Fixo • Cliente PPPoE
Interface LAN: • DHCP Avançado fixando IP ao MAC • Servidor DHCP • IP Fixo	**Segurança:** • NAPT • Server VPN: PPTP, L2TP e IPSEC • Client VPN: PPTP, L2TP e IPSEC • Firewall: Firewall Stateful, Configurações gerais, Filtros: DoS, Conteúdo e Usuários, Habilitar máquina DMZ
Configurações Gerais: • Gerenciamento WEB • Configuração das Portas: HTTPS, SSH e Telnet	**Filtros**: • Gerais: Bloqueio Messengers, Chat, ICQ, Peer-to-Peer, Trojan Horses, Traceroute: pacotes por UDP e ICMP. • DoS: SYN Flood, UDP Flood, ICMP Flood, Port Scan, Conexões por host, IP Options, Ping of Death, Smurf Attack e IP Spoofing. • Conteúdo: até 12 URLs bloqueadas • Usuário: até 12 regras de bloqueio por usuário

QoS: • Traffic Shaping • Marcação DSCP dos pacotes de áudio (RTP)	**Vídeo:** • Multicast – Triple Play e Túneis DVMRP
Gerência: • SNMP • Configurador Multiusuários	**NATT:** • STUN • UPNP-Cliente • FQDN Externo
Data/Hora: • NTP • RDATE	**Protocolos VoIP:** • SIP Integrado • SIP (Registrar/Proxy) • Cancelamento de eco automático G 168-2002 • Jitter Buffer de 20 ms a 80 ms (automático)
Codecs de Áudio: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps)	**Codecs para Fax:** G.711A (64kbps), G.711U (64kbps) e T.38
DTMF: dentro ou fora da banda	**Contas SIP:** até 1.000 contas **Contas SIP Integrado:** 64 contas
Ligações Simultâneas: 30 ligações (20 ligações G.729 e 10 ligações G.711)	**Linhas Digitais:** capacidade máxima de 30
Impedância (Porta Digital): 100 ohms	**Sinalização Digital R2/MFC:** • De linha: R2 digital ou R2 analógico (E M contínuo) • De registradores: entrada e saída MFC
E1 (R2 e ISDN): Master/Slave (Clock Regenerado)	**Proteção de Programação:** Memória não volátil FLASH
Alimentação AC: Entrada full-range: 95 Vac à 240 Vac	**Consumo Máximo:** 25 VA
Temperatura de Operação: 10ºC a 40ºC	**Umidade Relativa do Ar:** 20% a 90%
Falta de Energia: Deve ser adicionado No-break	**Instalação:** Mesa, Parede e [1]Rack 19" *[1]Opcional*
Dimensões (mm): A: 40 / L: 220 / P:130	**Peso Máximo:** 0,9 Kg
Bilhetagem: Via FTP	

1.3. Descrição do Hardware

1.3.1. Painel traseiro do Gateway Digistar

Descrição dos conectores do Gateway Digistar

Item	Descrição
PWR	Conector para entrada de alimentação (5 VDC)
WAN/ETH1	Conector Superior RJ-45
LAN/ETH0	Conector Inferior RJ-45
E1/T1	Conector E1/T1 RJ-45
CONSOLE	Entrada para console USB

1.3.2. Painel frontal do Gateway Digistar

Descrição dos LED's do Gateway Digistar

LED	Descrição
PWR	Ligado: quando a fonte do Gateway Digistar está funcionando.
VOIP	Piscando indica ligação VoIP ativa
LAN	Desligado indica "*link up" em* 10Mbps. Ligado indica "*link up" em* 100Mbps
	Piscando indica fluxo de dados pela porta. Ligado indica "*link up"*
WAN	Desligado indica "*link up" em* 10Mbps. Ligado indica "*link up" em* 100Mbps
	Piscando indica fluxo de dados pela porta. Ligado indica "*link up"*
E1	Link E1

2. Acessando o Configurador Web Digistar

Para perfeita funcionalidade, é recomendado sempre utilizar a versão mais recente do Browser.

Versão mínima para configurador WEB:

- Internet Explorer 8
- Firefox 15
- Safari 5
- Chrome 18
- Opera 11

As configurações do seu Gateway Digistar são realizadas através de páginas WEB que se encontram dentro do equipamento.

Inicialmente para acessar o Configurador Web Digistar, devemos conectar a interface de rede de um PC na interface LAN do Gateway Digistar. As interfaces de rede do Gateway Digistar são auto cross-over, ou seja, podem ser conectadas a qualquer cabo de rede.

Com a conexão correta, devemos configurar o PC para acessar a página. O PC deve ser configurado com gateway 192.168.10.1 e um IP nesta rede.

Após isto, acessaremos o Configurador Web Digistar. Para tanto, através de um WEB Browser, digitamos:

https://192.168.10.1

Observação:
As configurações feitas através de configurador WEB devem ser aplicadas para que tenham validade. Todas as páginas de configuração possuem um botão “Aplica”, e as alterações realizadas em cada página só serão validadas após o click neste botão. As alterações são gravadas em memória volátil tipo RAM, para que elas tenham efeito, gravar as configurações no campo “gravar” localizado na parte superior das páginas.

2.1. Login

Ao acessar a página, aparece a tela de logon, conforme abaixo:

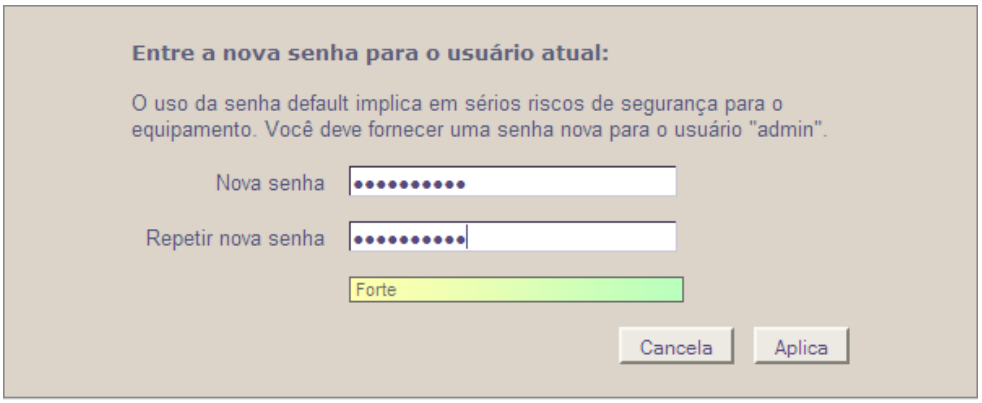
Nesta página o usuário “admin” e usuários autorizados podem optar pela configuração rápida ou configuração normal. Ao escolher a configuração rápida o usuário tem acesso somente às opções mais críticas para o funcionamento do Gateway Digistar. Esse modo foi criado para a primeira customização de uma máquina nova.
Atenção: Ao se encerrar o configurador rápido, todas as configurações atuais serão perdidas!

Para acessar, o usuário deve fornecer usuário e senha.

Usuário default: admin e senha default: admin

Usuário: até 20 caracteres
Senha: até 16 caracteres

OBS.: *No primeiro acesso do usuário admin com senha default, será requisitada a troca da senha deste usuário. O programa irá validar a senha entrada e indicará sua força com uma barra de progresso. O Botão Aplica só estará habilitado com uma senha forte.*


Entre a nova senha para o usuário atual:
O uso da senha default implica em sérios riscos de segurança para o equipamento. Você deve fornecer uma senha nova para o usuário "admin".
Nova senha
Repetir nova senha
Forte
Cancela
Aplica

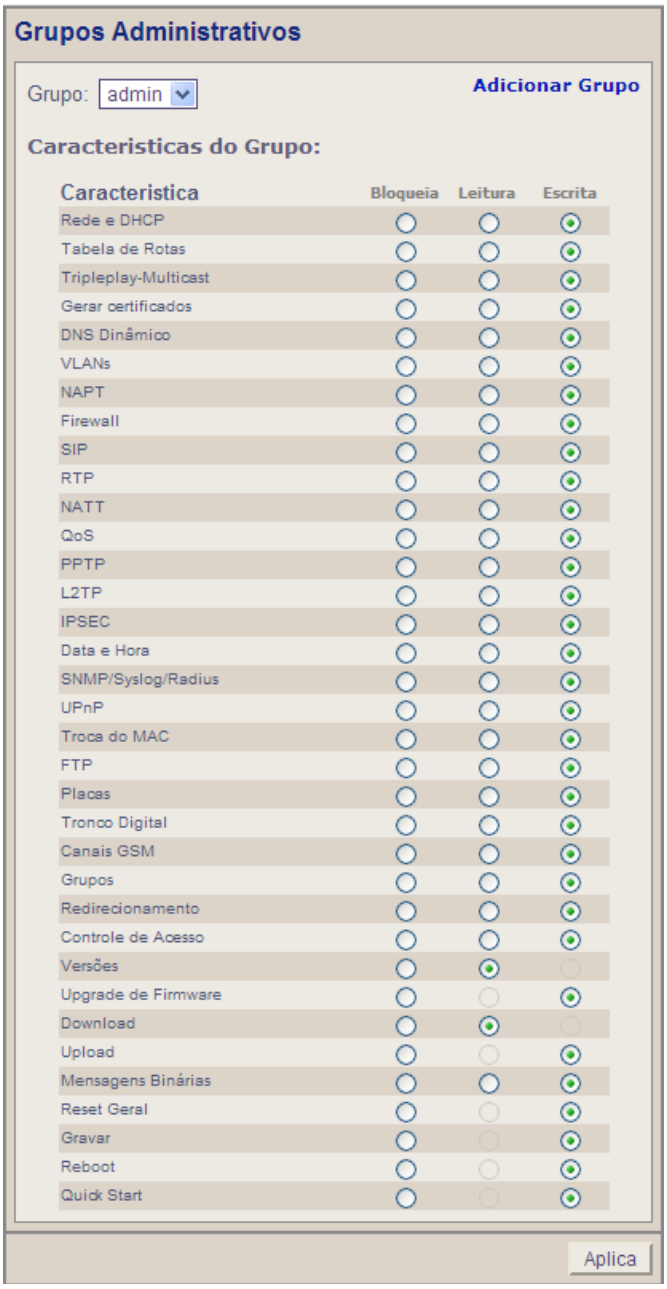
Após acessar o configurador com o usuário admin, aparece a tela abaixo:

O configurador WEB Digistar está disponível nos idiomas: Português, Inglês e Espanhol.

Nesta tela estão localizados um menu a esquerda e uma janela, que exibe algumas configurações de serviços configurados no Gateway Digistar. Estas configurações podem ser acessadas clicando-se sobre os “títulos” ou acessadas através do menu que se encontra no lado esquerdo da tela.

Cadastro Grupos de Usuários (Editar Grupos)

Com o usuário admin é possível cadastrar novos grupos de usuários (em Editar Grupos) e configurar os acessos de cada grupo.



Ao clicar em cima das palavras “Bloqueia”, “Leitura” ou “Escrita” habilita todos os itens.

Cadastro de Usuários (Editar Usuários)

Em “Editar Usuários” podem ser cadastrados os usuários com suas senhas. Cada usuário deve ser associado a um grupo de usuários, pois é lá que são definidas suas permissões.

Alteração da senha

Cada usuário, após logado, poderá alterar sua senha, clicando em “senha” que aparece no canto superior direito, conforme tela abaixo.

OBS.:

O tempo de inatividade do usuário admin é de 5min.

O tempo de inatividade dos demais usuários pode ser configurado. Os tempos disponíveis são: 1 min, 5 min, 10 min ou 15 min.

É permitido o cadastro de 8 grupos de usuários e 16 usuários.

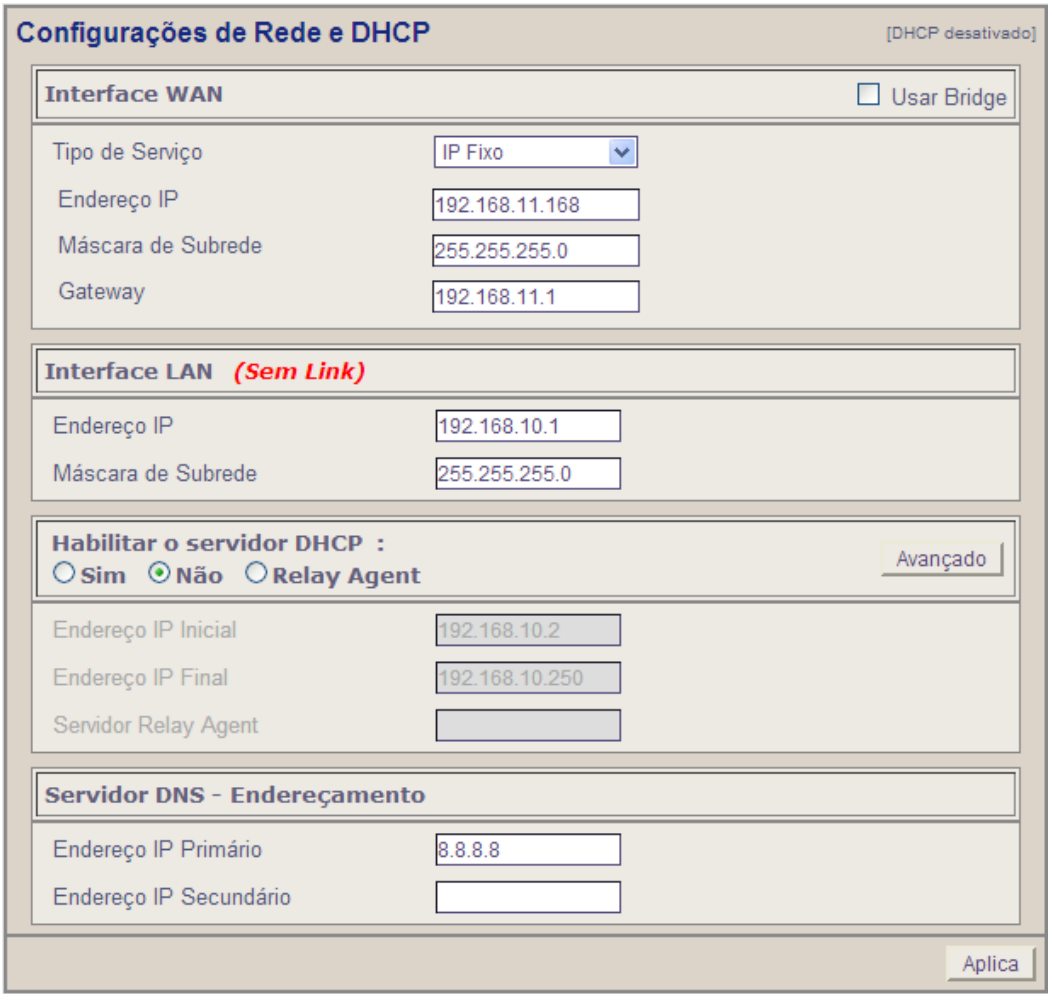
Não é permitido alterar os acessos do Grupo Admin.

3. Configurações de Sistema

3.1. Rede

Para usufruir o máximo de recursos de seu Gateway Digistar, é necessário que ele tenha um IP público da interface WAN, ou seja, que o Gateway Digistar esteja na "ponta da rede". Somente desta forma haverá o correto funcionamento de recursos como QoS, VPN e firewall, além de facilitar em muito a comunicação VoIP.

3.1.1. Configurações de Rede e DHCP



Interface WAN

A interface WAN tem 3 possibilidades de configuração:

- **Cliente DHCP:** DHCP significa *Dynamic Host Configuration Protocol*, ou seja, Protocolo de Configuração de Host Dinâmico. Em redes TCP/IP, todo computador precisa ter um número de IP diferente. Para que não haja conflito de duas máquinas terem o mesmo número IP, seleciona-se uma máquina que forneça os IPs para todas as máquinas da rede. Clicando na opção SIM para a interface WAN o endereço IP será obtido automaticamente. Esta é a opção padrão. Dependendo do servidor DHCP utilizado o endereço IP obtido pode mudar cada vez que o Gateway Digistar for religado.

> ***OBS.:*** *Se ligar o Gateway Digistar sem o cabo de rede, é necessário "Aplicar" as "Configurações de Rede e DHCP" após conectar o cabo para obter o endereço IP.*

- **IP Fixo:** Usa uma configuração de IP fixo. É normalmente usada quando não há servidores DHCP ou há a necessidade de fixar um IP dentro da rede. Para usar IP fixo devem ser configurados o endereço IP, a máscara de rede e o gateway (roteador).

- **Cliente PPoE :** Quando usado um modem bridge na interface WAN, existe a possibilidade do Gateway Digistar efetuar a autenticação. Para isso você deve entrar com o login, ou o nome do usuário e a senha. O protocolo de autenticação utilizado é PAP ou CHAP, selecionado automaticamente.
  Muitas vezes podem existir problemas na camada física em uma conexão do tipo PPPoE, que é de responsabilidade do modem externo. Assim, o link fica sem receber dados e o gateway não tem como saber se os dados pararam de chegar por inatividade ou por algum problema. Para resolver este problema foi implementado um comando de eco (echo em inglês) para que um pacote seja enviado pelo Gateway Digistar e o outro lado responda. Caso não seja recebida a resposta do eco, a interface do Gateway Digistar é reiniciada. Vale lembrar que nem todas as operadoras respondem ao echo. Também é possível configurar o intervalo de envio dos echos para ajustar o sistema.

Interface LAN

Endereço IP: Este endereço será o IP no qual se tem acesso ao configurador WEB a partir da interface LAN

O valor padrão da interface LAN é 192.168.10.1

Máscara de Subrede: Máscara de Sub-rede que deverá ser igual em todas as máquinas conectadas a porta LAN do Gateway Digistar. No Gateway Digistar este parâmetro define o número máximo de máquinas que podem ser conectadas na rede interna.

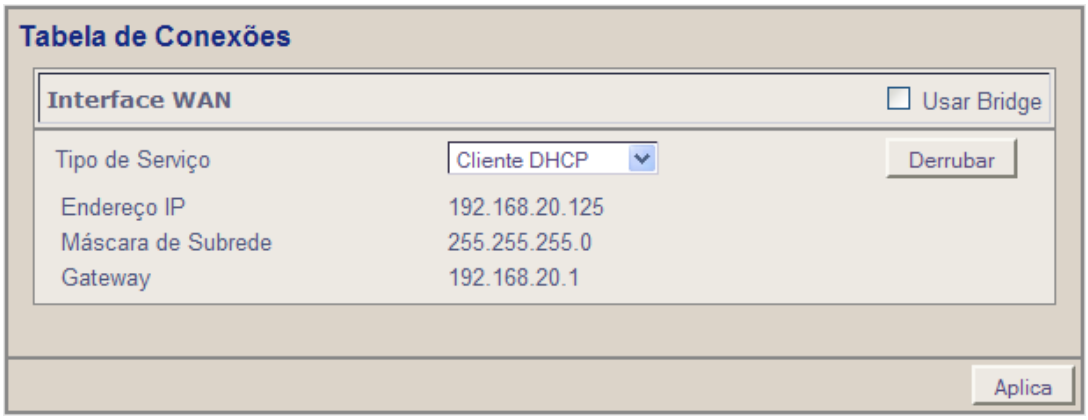
O valor padrão para a máscara de rede é 255.255.255.0 permitindo até 253 máquinas na rede interna do Gateway Digistar

Servidor DHCP

Para que as máquinas ligadas na LAN do Gateway Digistar possam usar IPs dinâmicos, o Gateway Digistar possui um servidor DHCP. Para configurar o servidor é necessário entrar com o endereço IP inicial e o endereço IP final que devem estar contidos no endereçamento da LAN.

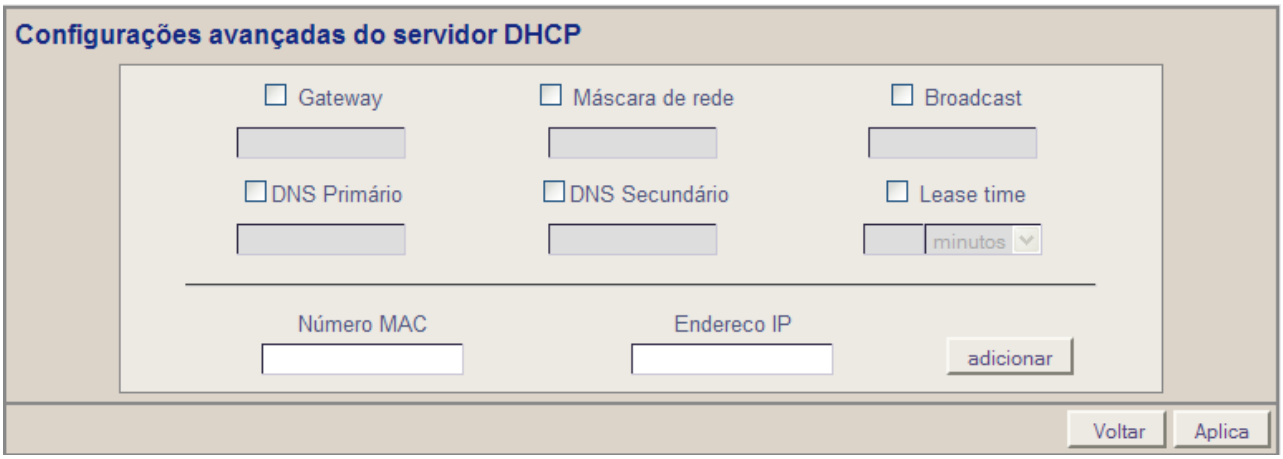
Caso alguma outra máquina dentro da mesma rede esteja fazendo o servidor DHCP é possível usar a opção DHCP *relay* onde é especificado o número IP desta máquina.

Existe a possibilidade de ver quais os IP que foram fornecidos pelo servidor DHCP. Clicando na opção "*Ver Tabela fornecida pelo DHCP"* mostra os números MAC de cada máquina com seus respectivos números IP.



DHCP Avançado

Além das configurações básicas como IP inicial e IP final do servidor DHCP, também é possível configurar, em "DHCP Avançado", o gateway, máscara de rede, broadcast, DNS primário e secundário, Lease Time (tempo de validade) e fixar o IP para cada número MAC.



Servidor DNS

Para transformar os nomes em endereços IP (p.ex www.digistar.com.br no IP 200.234.200.30), existem espalhados pela rede diversos servidores de nome. Existe a possibilidade de usar até dois servidores de nomes. O Gateway Digistar também pode ser utilizado como um DNS relay, desde que se configure nas máquinas da rede interna o DNS com o IP da LAN.

3.1.2. Configurações de Roteamento Estático

O processo de roteamento de pacotes da rede funciona de forma semelhante a uma ligação telefônica. Quando uma ligação é efetuada de uma origem até um destino a ligação passa por diversas centrais telefônicas. Se o número de destino não faz parte da central, a ligação é direcionada para outra central. Para que auxilie no processo existe uma série de códigos de operadoras, países, estados e cidades.

Bastante parecido com o processo das ligações telefônicas, ocorre o roteamento em uma rede de dados. Quando um dado é transmitido de uma origem até um destino, existem diversas máquinas na rede que estabelecem quais os caminhos que os mesmos devem percorrer. Estas máquinas são chamadas de *roteadores* ou *gateways* e o processo de decisão do caminho dos pacotes é chamado de roteamento.

Os roteadores possuem tabelas que contêm informações de quais redes e máscaras de redes que estão conectados a eles. Se a rede de destino especificada não estiver nas tabelas de rotas, os dados são encaminhados para uma rota padrão (*default* ou 0.0.0.0).

Existem dois tipos de roteamento: rotas estáticas e rotas dinâmicas. As rotas estáticas são explicitamente configuradas pelo usuário, e as rotas dinâmicas podem ser "aprendidas" e divulgadas através da utilização de protocolos especiais.

No Gateway Digistar o usuário pode configurar as rotas estáticas de duas formas: como host ou como rede. Deve-se usar uma rota do tipo *host* quando houver a conexão de uma máquina isolada na rede LAN do Gateway Digistar. Quando houver outra rede na LAN do Gateway Digistar, deve-se adicionar uma rota do tipo rede para que os dados sejam roteados corretamente.

A rota padrão do Gateway Digistar é sempre a conexão da WAN, quer ela esteja configurada como dinâmica, estática ou PPPoE.

Para visualizar as tabelas de roteamento que estão ativas, basta clicar na opção "*Ver Tabela de Roteamento*"

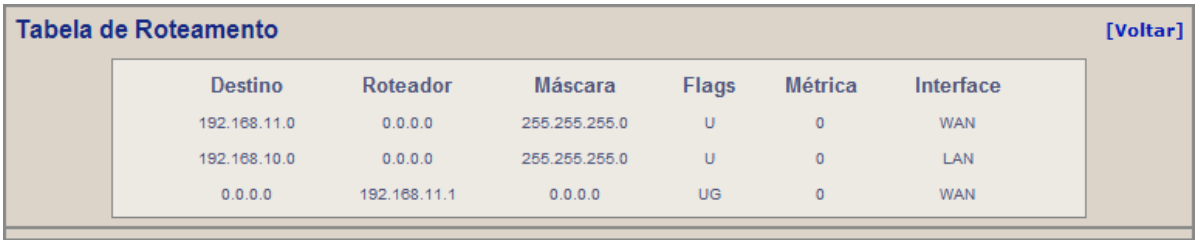
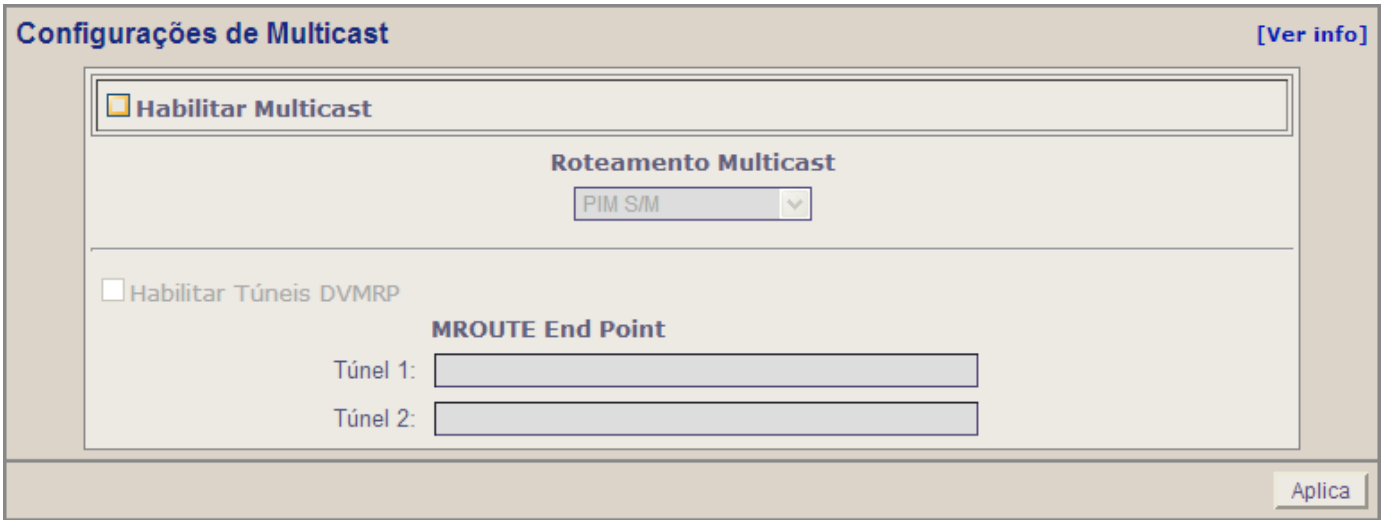


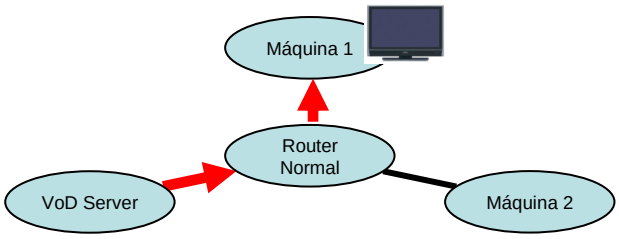
Tabela de Roteamento
[Voltar]
Destino Roteador Máscara Flags Métrica Interface
192.168.11.0 0.0.0.0 255.255.255.0 U 0 WAN
192.168.10.0 0.0.0.0 255.255.255.0 U 0 LAN
0.0.0.0 192.168.11.1 0.0.0.0 UG 0 WAN

OBS.: *As métricas são automáticas.*

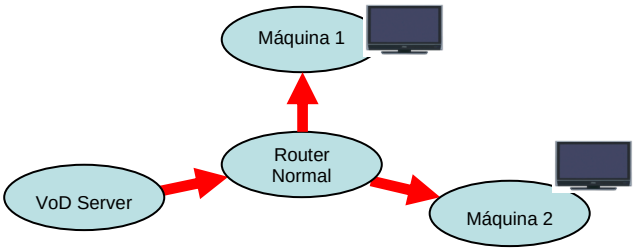
3.1.3. Configurações de Multicast



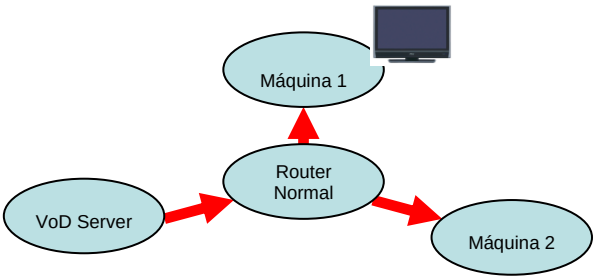
Multicast - Triple Play: O triple play é a união de dados, voz e vídeo na Internet. O Gateway Digistar faz somente redirecionamento dos pacotes de vídeo, não fazendo transcodificação (mudança de padrão) ou redimensionamento. Atualmente os vídeos utilizam pacotes do tipo Unicast. Abaixo podemos ver uma máquina de Vídeo sobre Demanda (VoD) transmitindo para a Máquina 1:



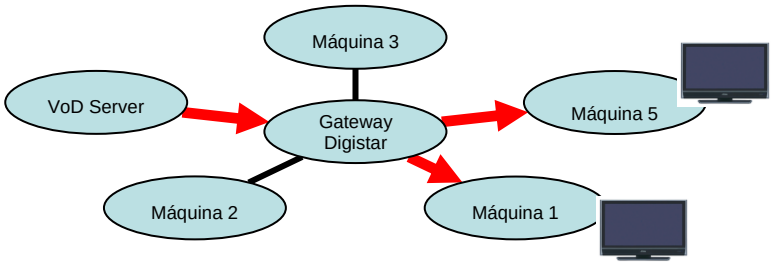
Para a Máquina 2 ver o vídeo, o VoD tem que transmitir o dobro de banda para as duas máquinas poderem assistir o vídeo.



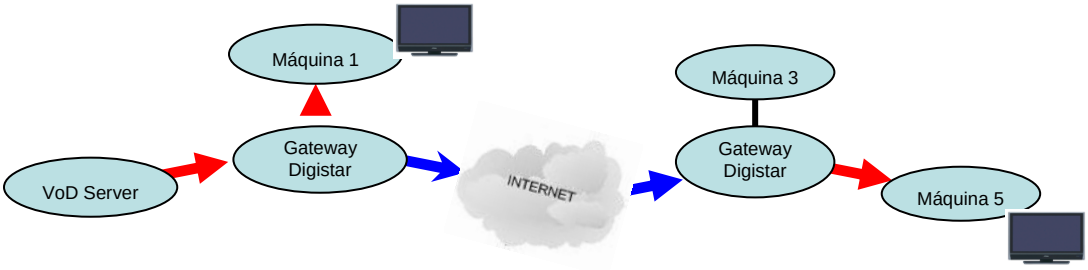
Outra alternativa para economizar banda do VoD seria utilizar pacotes do tipo broadcast. Todas as máquinas do roteador estariam recebendo vídeo, querendo ou não vê-los.



Com o Multicast podemos economizar banda do servidor de vídeo e mandar apenas para quem precisa:



Isso viabiliza sistemas de vídeo-conferência, vídeo-aula, treinamentos on-line e IPtv. Atualmente poucos roteadores no mercado suportam multicast assim como a própria WEB. A Digistar, já preparando seu Gateway para a necessidade de transmissão de vídeo pela WEB, tem como recurso os túneis DVMRP, que capturam os pacotes multicast para serem enviados unicast para outro roteador.



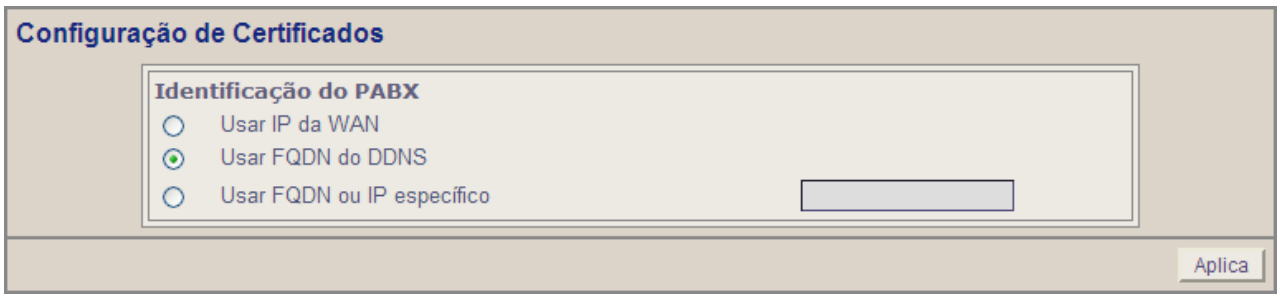
3.1.4. Configuração de Certificados

Certificados digitais são arquivos que tem o propósito de identificar realmente cada máquina. Em um certificado digital há informações pessoais da empresa, mas a principal informação presente em um certificado é a sua chave pública. A criptografia usada na Internet se baseia no sistema de chaves. O algoritmo usado na criptografia faz com que sejam geradas duas chaves, uma pública e outra privada. A chave pública, que está presente no certificado digital, é usada para criptografar dados a serem enviados ao dono do certificado. Já a chave privada, que só o dono do certificado conhece, serve para descriptografar a informação que foi criptografada com a sua chave pública. É importante notar que não é possível descriptografar a informação sem ter a chave privada e não há meios de, através da chave pública, deduzir a chave privada.

Outro ponto importante para a geração do certificado é a identidade de cada Gateway Digistar, chamado de nome comum. O nome comum é o endereço do Gateway Digistar. É importante lembrar que para a geração de certificados não existe a tradução de nomes para endereços, ou seja, se o nome comum do certificado for "www.digistar.com.br" o certificado só será válido se o usuário digitar especificamente o nome "www.digistar.com.br". Se for digitado o IP correspondente ao site www.digistar.com.br, que é 200.234.200.30, irá aparecer uma mensagem indicando um erro no certificado.

Cada nome na internet também é chamado de FQDN, ou Nome de Domínio Totalmente Qualificado e pode ser configurado com seu IP fixo através de um provedor de nome (DNS providers) ou até mesmo com IP dinâmico através de provedores de DNS dinâmicos (ver *"seção abaixo"*).

Como cada Gateway Digistar terá um FQDN ou IP diferente, é necessário criar um certificado próprio para garantir mais autenticidade e segurança.



3.1.5. Configurações do DNS Dinâmico

A internet com IPv4 utiliza endereçamento de 4 octetos em que cada um pode ir de 0 a 255. Assim para cada máquina conectada temos que ter um número do tipo 200.200.200.200. Uma solução para que não precisássemos saber o número IP de cada site na internet foi usar um servidor de nomes que faz a troca de endereços do tipo *www.digistar.com.br* para 200.234.200.30.

Em alguns casos, os números IP fornecidos pelos servidores DHCP da WAN ou pelo provedor no PPPoE podem mudar em intervalos de tempo. Se houver uma troca de número IP, a associação com o nome irá falhar.

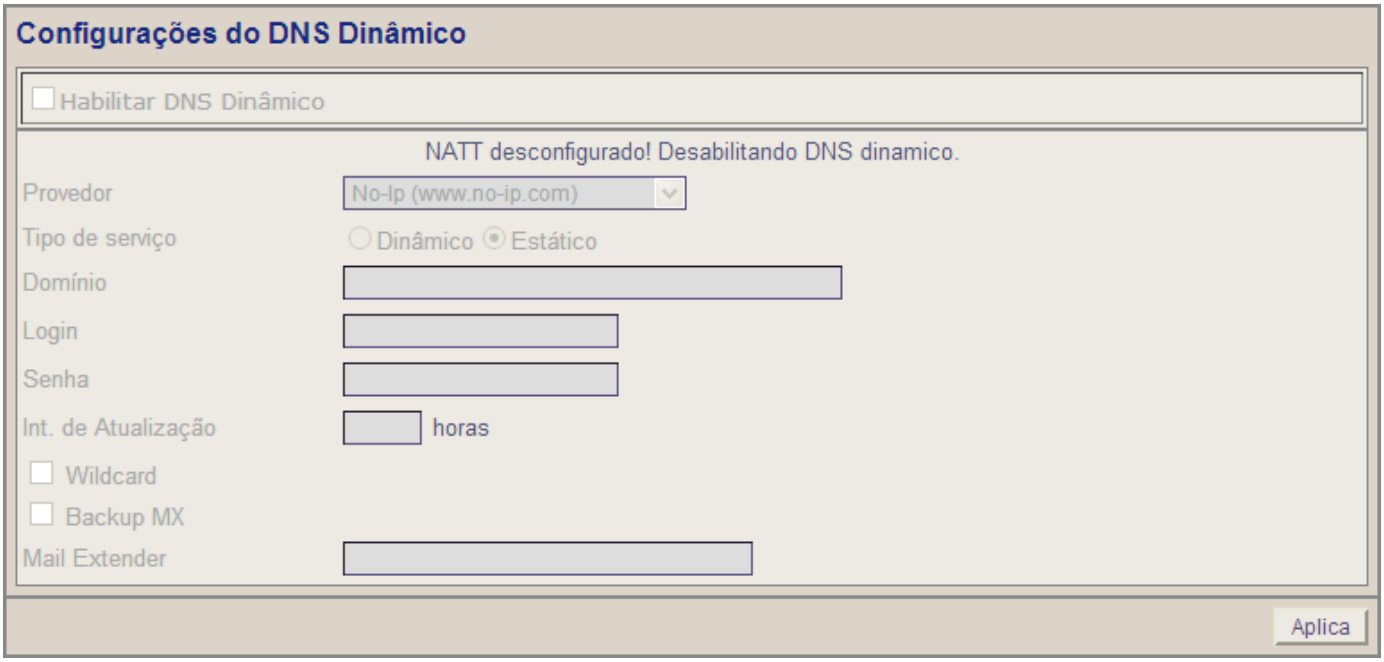
Para resolver estes problemas alguns provedores oferecem serviços conhecidos como DNS dinâmicos. Estes serviços registram um nome associando ao IP fornecido pela operadora. Em intervalos de tempo ou toda vez que houver uma troca de IP, todos os servidores de nome da internet serão atualizados. Se você possuir um IP fixo, também é possível configurar o Tipo do Serviço como estático, assim só haverá atualização de registro quando o Gateway Digistar for ligado.

Normalmente os servidores de nomes fornecem um nome do tipo *nome.servidor.com*. É possível usar um wildcard (coringa) na frente do nome, assim qualquer coisa na frente do nome.servidor.com é vista como um sinônimo. Por exemplo, se for marcado o wildcard, o domínio *www.servidor.no-ip.com*, *www2.nome.servidor.no-ip.com* ou *nome.servidor.no-ip.com* são sinônimos, ou seja, fornecem o mesmo número IP.

Também existe a opção de redirecionar os e-mails recebidos no *mail.nome.servidor.no-ip.com*, de acordo com nosso exemplo, para outro servidor de e-mails, caso o Gateway Digistar estiver desligado. Para isso, basta ligar a opção backup MX, especificando onde os e-mails serão guardados. Todas as opções devem ser suportadas pelos provedores de DNS dinâmico.

Se o Gateway Digistar estiver atrás de um NAPT, ou seja, possuir um IP privado na interface WAN, o DNS dinâmico será automaticamente desabilitado. Alternativamente é possível usar o DNS dinâmico com a opção STUN do NATT (*Ver "Configuração do NATT"*). Usando o STUN, o Gateway Digistar irá descobrir qual o IP externo para mandar para o servidor DDNS.

Dependendo do intervalo de tempo em que o endereço da WAN sofre atualizações, é possível atualizar o endereço com o FQDN (nome do domínio completo) no Intervalo de Atualização de 0.1 horas (6 minutos) à 99 horas.

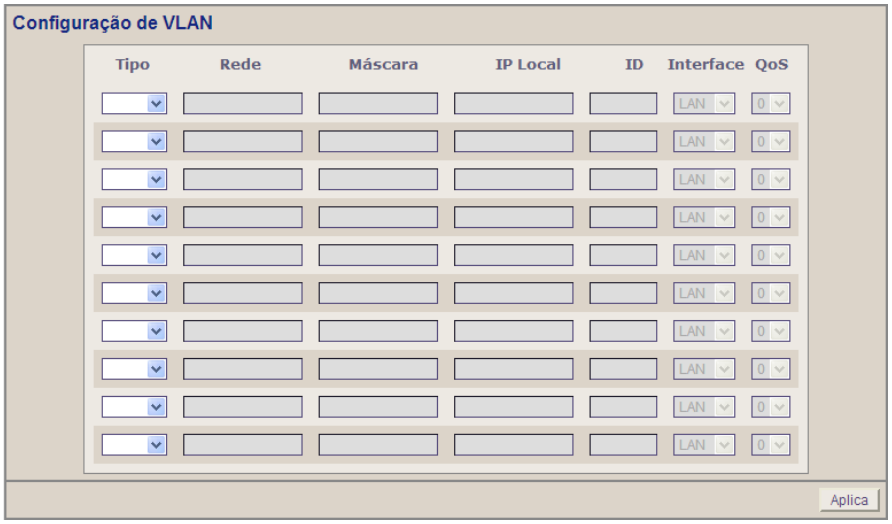


3.1.6. Configuração de VLAN

O nome VLAN é uma abreviatura de Rede de Acesso Local Virtual. A principal vantagem é de computadores ligados em locais físicos diferentes se comportarem como se estivessem conectados no mesmo fio. A configuração de VLANs é feita por software, tornando as redes extremamente flexíveis, assim um computador pode se mover para outro local físico (dentro da mesma LAN) sem a necessidade de nenhuma mudança de configuração de hardware ou software.

As VLANs são definidas pela IEEE 802.1Q operando em camada 2 pelo modelo OSI. Porém como cada definição de VLAN mapeia uma rede e sub-rede, existe a impressão de estar trabalhando em camada 3, a nível de rede. Reduzindo o tamanho das redes, reduzimos também o tamanho de domínio de broadcast.

É possível criar dentro de cada LAN até 4096 VLANs (ID). Cada VLAN também tem oito possibilidades de priorização de pacotes no campo QOS. As VLANs podem ser do tipo host (para ligar apenas uma máquina) ou do tipo rede (para criar realmente uma rede virtual). As VLANs podem ser criadas dentro da rede interna (LAN) ou para a interface externa (WAN).

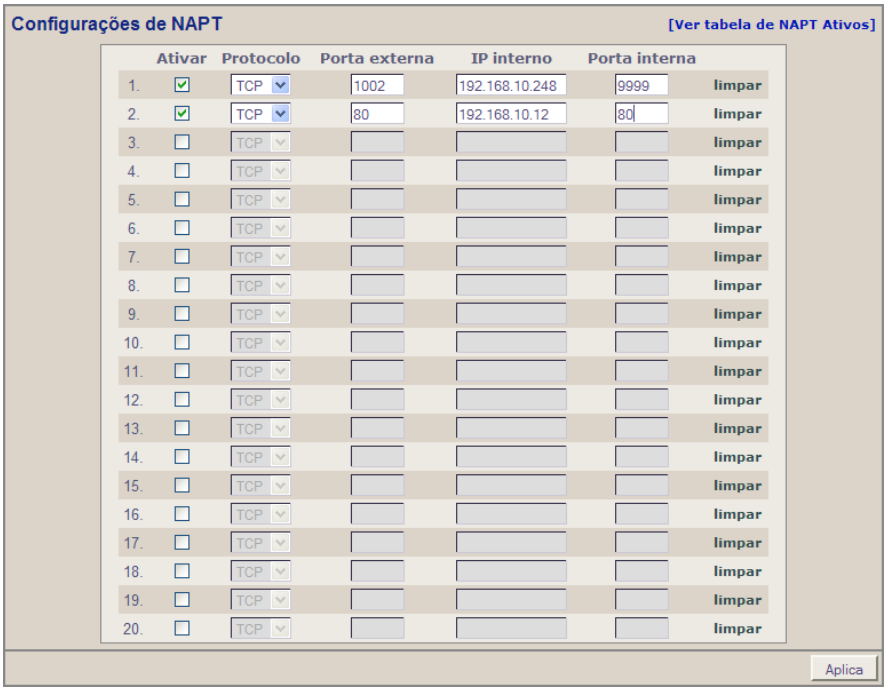


3.1.7. Configurações de NAPT

NAPT (Network Address and Port Translation) é a tradução de endereços e portas de rede, sendo ambos utilizados para mapear endereços e/ou portas de uma rede interna para um IP público real. NAT/PAT também é uma ferramenta de proteção contra ataques, uma vez que as máquinas conectadas na rede interna não são visíveis à rede externa.

De maneira geral o uso do NAT/PAT se dá de forma automática e transparente. Um computador ligado à rede interna (LAN) do Gateway Digistar pode fazer um acesso externo sem qualquer problema.

Em alguns casos, existe a necessidade de instalar um servidor em uma máquina na rede interna. Isso é muito utilizado em servidores de página WEB ou servidores de e-mail. Para isso é possível especificar qual a translação do IP e/ou a porta do serviço externo para uma máquina interna.



Por exemplo, se existe um servidor http (WEB) na porta 80 da máquina 192.168.10.12 conectada na rede LAN do Gateway Digistar é possível criar uma regra:

Protocolo – TCP (para servidor http), porta externa - 80, IP interno 192.168.10.12 (IP da máquina na rede interna que possui o serviço) e porta interna 80 (a porta utilizada pelo serviço).

Com o exemplo acima, toda vez que for acessado o IP externo a WAN na porta 80, o Gateway Digistar fará uma conexão com a máquina interna 192.168.10.12.

3.2. Firewall

Um firewall tem a tarefa de restringir o tráfego entre uma **rede protegida** e uma **rede não-confiável.** Este procedimento visa aumentar a segurança da rede protegida, minimizando a possibilidade de atividade maliciosa. Porém, deve-se notar que qualquer serviço cujo acesso seja permitido através do firewall ainda é um risco potencial. As abordagens utilizadas para segurança de uma rede em ordem crescente de grau de limitação de tráfego são descritas abaixo:

Tudo é permitido: Permite todo tráfego de rede, ou seja, não existe proteção.

Tudo que não é proibido é permitido: Proíbe explicitamente determinados tráfegos. Todo o resto do tráfego é permitido. É difícil determinar todos os tipos de tráfego potencialmente maliciosos.

Tudo que não é permitido é proibido: Permite explicitamente determinados tráfegos. Todo o resto do tráfego é proibido. O tráfego que deve ser permitido é mais fácil de determinar que o tráfego que não deve ser permitido. Se o tráfego não for explicitamente permitido será bloqueado.

Tudo é proibido: Sem tráfego entre a rede protegida e a rede não-confiável. Utilizada por exemplo em casos de suspeita de invasão.

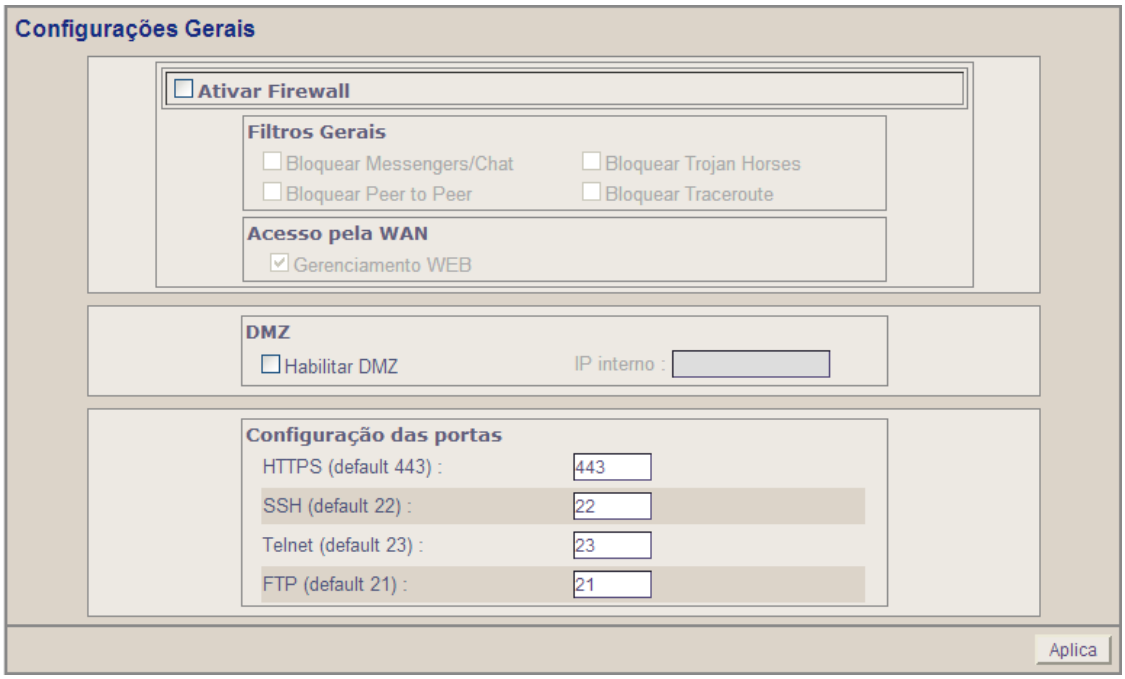
A abordagem utilizada pelo firewall implementado no Gateway Digistar é a **tudo que não é permitido é proibido.** Este é o tipo de firewall mais recomendado e utilizado por ser o mais seguro. A rede protegida engloba as máquinas acessíveis pela interface da LAN e por túneis VPN. A rede não-confiável é formada pelas máquinas acessíveis pela interface da WAN. O firewall do Gateway Digistar é um firewall stateful, ou seja, guarda o estado do tráfego recente de pacotes. Por padrão o firewall ativado permite os seguintes tipos de tráfego:

- Pacotes originados da rede protegida para qualquer destino.
- Pacotes TCP de conexões já estabelecidas ou sendo iniciadas pela rede protegida.
- Pacotes UDP onde já houve tráfego em alguma das direções.
- Pacotes ICMP relacionados a outros pacotes.
- Pacotes ICMP echo-request.
- Pacotes TCP e UDP para portas explicitamente abertas.
- Outros tráfegos explicitamente permitidos, determinados pelas configurações dos serviços Gateway Digistar.

As configurações do firewall pela interface Web estão divididas em quatro páginas. A primeira página contém configurações gerais e as páginas seguintes as configurações para proteção contra ataques de DoS, regras de firewall do usuário e filtros de conteúdo. Para que o firewall possa estar ativo é necessário que a interface da WAN esteja configurada.

3.2.1. Configurações Gerais

Nesta página pode ser ativado/desativado o firewall e configurar o acesso a serviços pela interface da WAN.



Ativar Firewall: Ativa/Desativa o Firewall. A ativação ou desativação afeta as configurações das demais páginas do firewall, ou seja, para que as configurações das outras páginas do firewall tenham efeito, o firewall deve estar ativado aqui.

- **Filtros Gerais:** permitem bloquear determinados tráfegos de dados.
  - Bloquear Messengers/Chat: protocolos de troca de mensagens instantâneas como ICQ e MSN Messenger.
  - Bloquear Peer-to-Peer: protocolos peer-to-peer de compartilhamento de arquivos como pelas redes eDonkey, Kazaa e BitTorrent.
  - Bloquear Trojan Horses: portas comuns de cavalos de Tróia. As portas TCP bloqueadas são: ”135 à 139, 444, 666, 1234, 1524, 3127 à 3149, 4000, 6000, 6006, 12345, 12346, 16660, 27665, 31337, 33270". As portas UDP são: ”135 à 139, 444, 995, 996, 997, 998, 999, 6667, 6711, 8998, 12345, 12346, 27444, 31335, 31337, 60001”.
  - Bloquear Traceroute: pacotes de traceroute por UDP e ICMP.

- **Acesso pela WAN:**
  - Gerenciamento WEB: Habilita/Desabilita o acesso ao Configurador Web Digistar pela interface da WAN. Se estiver desabilitado então o gerenciamento só pode ser realizado a partir da rede protegida.

- **Habilitar DMZ:** Especifica uma máquina da rede protegida para ser utilizada como DMZ (De-Militarized Zone). Se o DMZ estiver habilitado os pacotes serão tratados respeitando a seguinte ordem de precedência:
  - Pacotes para portas abertas pelo Gateway Digistar não são redirecionados.
  - Pacotes para portas com redirecionamento por NAT são enviados para as máquinas da rede protegida correspondentes ao redirecionamento.
  - Pacotes para as demais portas são redirecionados para a máquina configurada como DMZ.

- **Configuração das Portas:**
  - HTTPS: especifica a porta que será utilizada pelo servidor https do Configurador. Por padrão é utilizada a porta 443. No caso de alteração desta porta, a página do configurador deve ser recarregada no browser especificando a nova porta.

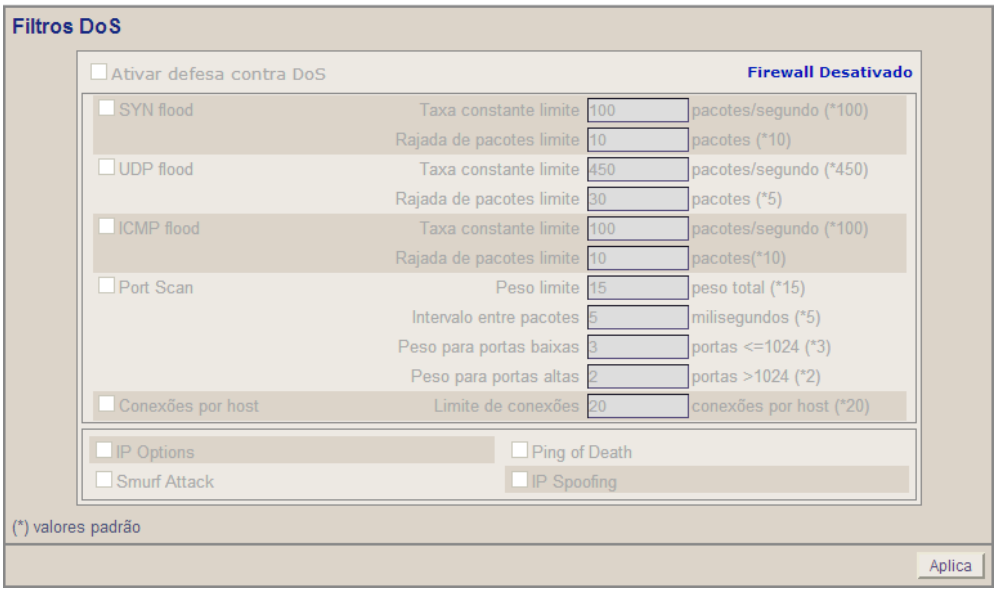
  - SSH: É utilizada para fins de depuração do equipamento. Se em sua rede há algum servidor SSH, para que esta porta (padrão 22) seja redirecionada pelo NAPT ou DMZ, há a necessidade de trocar a porta SSH do Gateway Digistar para outra diferente da porta 22.

  - Telnet: É utilizada para fins de depuração do equipamento. É semelhante ao protocolo SSH, mas este não possui criptografia. Se em sua rede há algum servidor telnet, para que esta porta (padrão 23) seja redirecionada pelo NAPT ou DMZ, há a necessidade de trocar a porta SSH do Gateway Digistar para outra diferente da porta 23.

  - FTP: especifica a porta que será utilizada pelo servidor FTP para consulta de bilhetagem. Usuário e senha do FTP são configurados na tela Servidor FTP em "Serviços".

3.2.2. Filtros DoS

Nesta página são feitas as configurações de proteção contra ataques comuns de DoS (*Denial of Service ou Negação de Serviço*). Ataques deste tipo comprometem a disponibilidade das máquinas atingidas, seja por alguma vulnerabilidade de segurança ou por sobrecarga de processamento, fazendo com que estas não consigam atender a demanda de requisições dos clientes. As configurações a seguir devem ser utilizadas com cautela sob o risco de comprometer a eficiência da rede ou mesmo torná-la inutilizável através do Gateway Digistar. Deve-se tomar cuidado, sobretudo, com as configurações de proteção contra flood e limite de conexões. Caso deseje alterar os parâmetros pré-configurados para as configurações dos filtros DoS é recomendado que se verifique se o desempenho da rede não foi prejudicado antes de salvar as configurações. Cada configuração de filtro DoS possui parâmetros, com valores padrão que podem ser utilizados com segurança.


Filtros DoS
Ativar defesa contra DoS
Firewall Desativado
SYN flood
Taxa constante limite 100 pacotes/segundo (*100)
Rajada de pacotes limite 10 pacotes (*10)
UDP flood
Taxa constante limite 450 pacotes/segundo (*450)
Rajada de pacotes limite 30 pacotes (*5)
ICMP flood
Taxa constante limite 100 pacotes/segundo (*100)
Rajada de pacotes limite 10 pacotes(*10)
Port Scan
Peso limite 15 peso total (*15)
Intervalo entre pacotes 5 milisegundos (*5)
Peso para portas baixas 3 portas <=1024 (*3)
Peso para portas altas 2 portas >1024 (*2)
Conexões por host
Limite de conexões 20 conexões por host (*20)
IP Options
Ping of Death
Smurf Attack
IP Spoofing
(*) valores padrão
Aplica

- **Ativar defesa contra DoS:** Ativa/Desativa as configurações de defesa contra DoS.
  Os filtros de proteção contra flood se baseiam em algoritmos de baldes de fichas (token bucket algorithms), bastante utilizados para controle de tráfego em dispositivos roteadores. A implementação do algoritmo permite configurar a taxa limite para rajadas de pacotes (limit burst) e o valor para taxas constantes de pacotes (limit rate). No caso de suspeita de flood é gerado log com informações. Para pacotes TCP SYN, os pacotes originados da máquina suspeita são descartados durante 10 segundos.

SYN Flood: Limita a entrada dos pacotes TCP com flag SYN setada. Este tipo de pacote é utilizado para iniciar uma conexão TCP. Como cada recebimento de pacotes SYN acompanha a alocação de estruturas de dados para posterior estabelecimento da conexão TCP, um flood destes pacotes acabaria consumindo muitos recursos do sistema. Para minimizar este problema uma solução é descartar pacotes SYN excessivos originados de uma mesma máquina.

UDP Flood: Descarta pacotes UDP originados de uma mesma máquina em caso de suspeita de flood para evitar sobrecarga do sistema.

ICMP Flood: Descarta pacotes ICMP originados de uma mesma máquina em caso de suspeita de flood para evitar sobrecarga do sistema.

Port Scan: Proteção contra as técnicas de port scan mais conhecidas como TCP SYN, TCP connect, UDP, Stealth FIN, Xmas e Null Scans. Estes tipos de técnicas servem para encontrar portas abertas em máquinas e são os passos iniciais para a maioria dos ataques. Em caso de suspeita de port scan, o tráfego com a máquina remota é interrompido por 10 segundos e é gerado log com as informações. Quando um pacote de port scan é recebido na interface da WAN é criado um contador associado ao IP da máquina originadora deste pacote. Os pacotes de port scan seguintes originados desta mesma máquina incrementam o contador. Considera-se que o IP de origem está tentando realizar um port scan caso o contador atinja um valor limite pré-determinado. O mecanismo para detecção de port scan é configurado com os parâmetros a seguir:

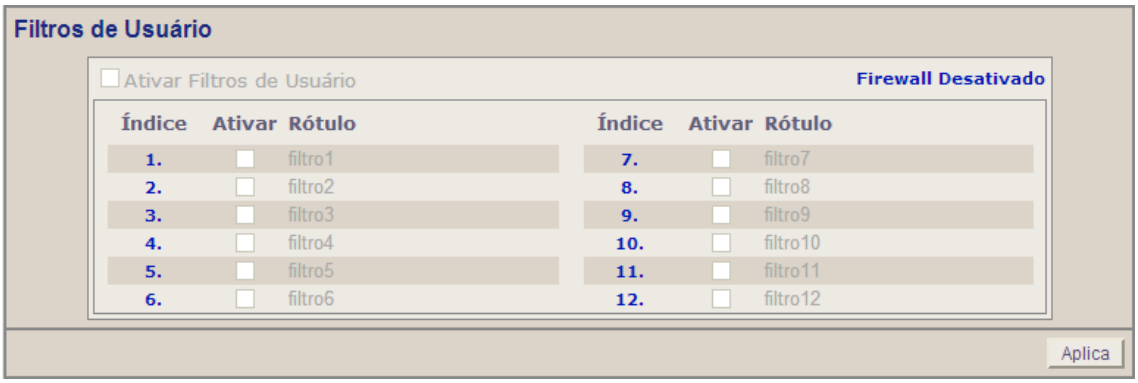
- **Peso limite**: Valor limite do contador.
- **Intervalo entre pacotes**: Intervalo máximo de tempo, em centésimos de segundo, entre dois pacotes com portas diferentes e mesmo IP de origem para que o último pacote possa ser considerado um pacote de port scan.
- **Peso para portas baixas e para portas altas:** Os port scans são mais comuns em portas baixas (menores ou iguais a 1024), onde estão as portas padrão dos serviços mais visados por atacantes. Por causa desta tendência em ataques a portas mais baixas, o mecanismo de detecção permite especificar pesos distintos para pacotes destinados a portas baixas e para portas altas. Este peso é o valor que é acrescido ao contador do IP da máquina origem para cada potencial pacote de port scan recebido nas portas baixas, menores ou iguais a 1024, ou nas portas altas, maiores que 1024.

Por exemplo, considere que a proteção para port scan está habilitada e configurada com os seguintes parâmetros: peso limite igual a 15, intervalo entre pacotes igual a 5, peso das portas baixas igual a 4 e peso das portas altas igual a 3. Suponha a tentativa de port scan pela técnica TCP Stealth FIN a seguir: A máquina 10.20.30.40 envia uma seqüência de 5 pacotes para o IP da WAN do Gateway Digistar em cada uma das portas no intervalo de 21 a 25. O intervalo de tempo entre os envios é de 4 centésimos de segundo. Este intervalo está dentro do intervalo máximo configurado, então o contador será incrementado para cada um destes pacotes recebidos pela WAN do Gateway Digistar. O valor de cada incremento será de 4 unidades, pois todos os pacotes são para portas baixas. Com isso o contador para o IP 10.20.30.40 irá atingir o peso limite no quarto pacote de port scan recebido. A tentativa de port scan será registrada em log e os pacotes originados de 10.20.30.40 serão descartados durante 10 segundos.

- **Conexões por host:** Limita o número de conexões TCP entre o Gateway Digistar e cada IP de máquina remota. Tentativas de novas conexões além do limite são ignoradas.
- **IP Options:** Descarta pacotes IP com IP Options setadas. Estes tipos de pacotes podem ser utilizados para comprometer sistemas com vulnerabilidades no protocolo IP.
- **Ping of Death:** Proteção contra pacotes ping of death. Pacotes icmp com tamanho muito grande. Alguns sistemas como o Windows 95 possuem vulnerabilidades a esse tipo de ataque. Para proteger as máquinas da LAN do Gateway Digistar os pacotes ICMP com tamanho muito grande são descartados.
- **Smurf Attack:** Protege contra ataques Smurf. Pings em broadcast com spoofing no IP de origem. Neste tipo de ataque o atacante envia pacotes ICMP echo-request em broadcast para uma subrede com IP de origem falsificado com o IP da vítima. Assim a vítima receberá tantos ICMP echo-replies quantas forem as máquinas da subrede que responderem ao ICMP echo-request. Esta subrede é chamada de smurf amplifier. Dependendo do número de máquinas na subrede e do número de ICMP echo-requests enviados pelos atacantes o acesso à máquina vítima poderá ficar comprometido. Para evitar que este tipo de ataque utilize a subrede do Gateway Digistar como smurf amplifier os pacotes ICMP em broadcast são descartados.
- **IP Spoofing:** Protege contra IP spoofing. Esta técnica consiste na alteração do IP de origem de pacotes fazendo que uma máquina atacante se passe por outra máquina. Diversos tipos de ataque são realizados em conjunto com IP spoofing, dentre elas o Smurf Attack. Para minimizar esses tipos de ataque o Gateway Digistar pode utilizar a técnica de reverse path filtering. O reverse path filtering verifica se a rede do IP de origem de cada pacote é alcançável pela interface que o pacote foi recebido, caso não seja o pacote é descartado.

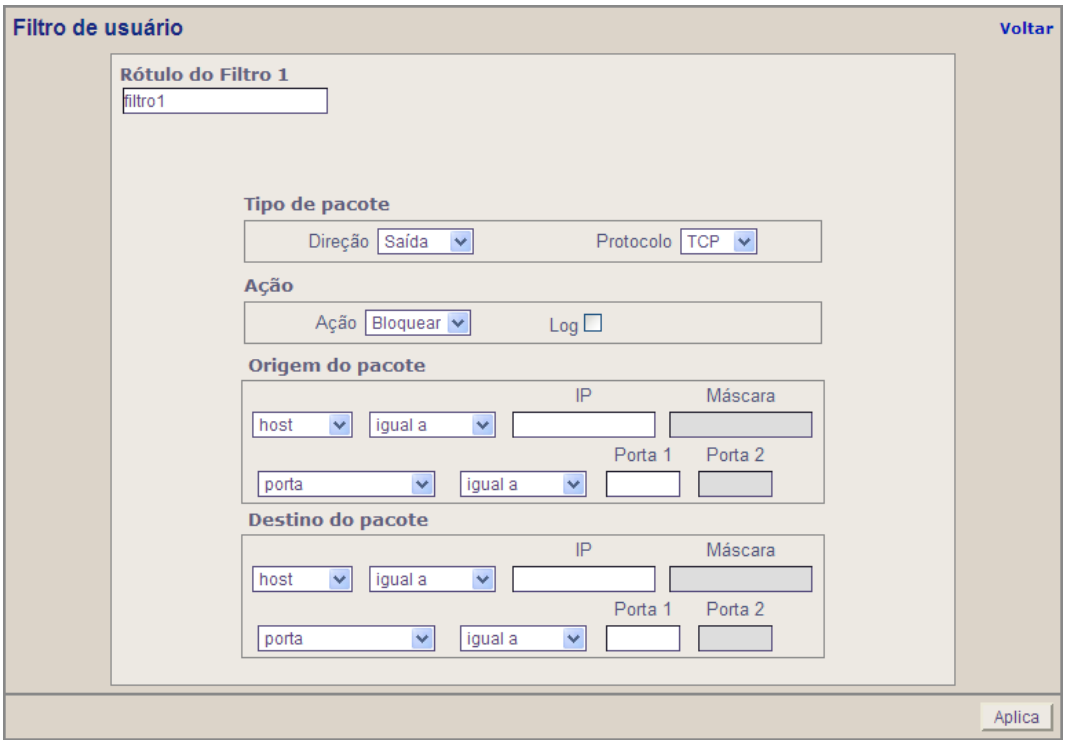
3.2.3. Filtros de Usuário

Os filtros de usuário permitem que o usuário especifique suas próprias regras de firewall. Na versão atual do firewall é possível adicionar até 12 regras que serão cascateadas, uma após a outra.



O casamento de pacotes IP é feito pelo **tipo, origem** e **destino** do pacote. Pelo tipo indica-se a **direção** do pacote, ou seja, se ele está entrando na interface da WAN ou saindo por ela, e o **protocolo**, que pode ser TCP, UDP, ICMP ou IGMP.

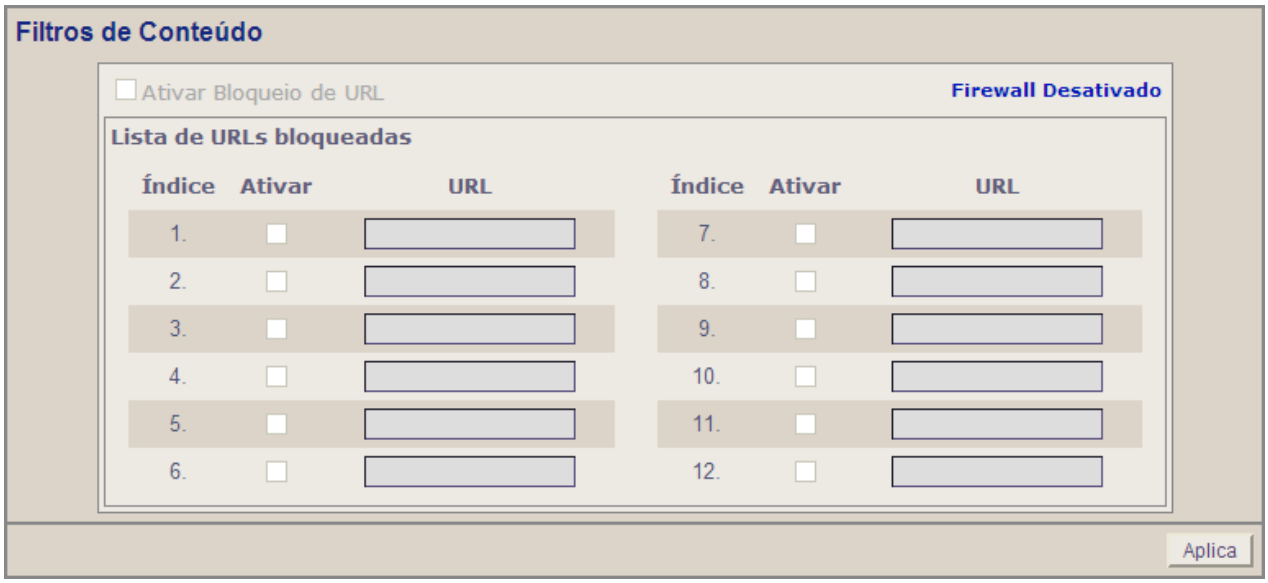
Pela origem e pelo destino pode-se indicar a máquina ou subrede e, no caso dos protocolos UDP e TCP, também podem ser informadas as portas utilizadas pelos pacotes. Quanto mais informações forem fornecidas, mais restrita será a regra. Quanto mais informações forem omitidas, mais ampla será a regra. Por exemplo, a regra que aceita pacotes TCP entrando na WAN da subrede 10.20.30.0 com máscara 255.255.255.0 é mais ampla que a regra que aceita pacotes TCP entrando na WAN da subrede 10.20.30.0 com máscara 255.255.255.0 com portas de destino entre 10000 e 20000. A primeira regra além de casar com os pacotes que casariam com a segunda regra também casa com pacotes com porta origem fora do intervalo de 10000 a 20000.



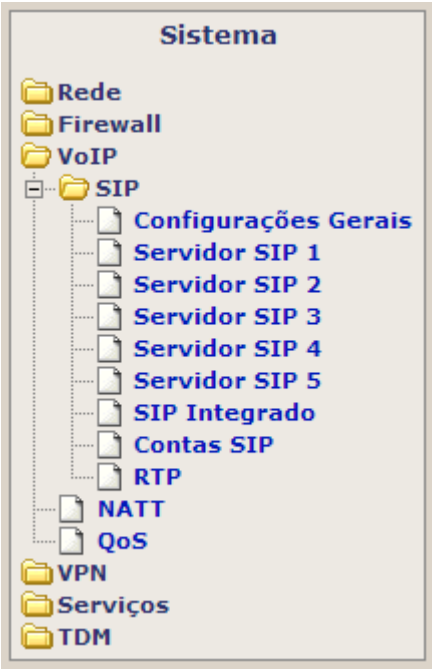
No caso de um pacote casar com alguma regra, a **ação** correspondente é executada e as demais regras são ignoradas. As ações possíveis são aceitar ou bloquear o pacote. Opcionalmente pode-se gerar **log** para cada pacote trafegado que casa com a regra criada.

3.2.4. Filtros de Conteúdo

Os filtros de conteúdo oferecem bloqueio de URLs para serviços de http. Até um total de 12 URLs podem ser bloqueadas. Para utilizar este recurso, basta adicionar a URL desejada e ativar a regra. Todas as requisições para URLs bloqueadas serão descartadas.



3.3. VoIP



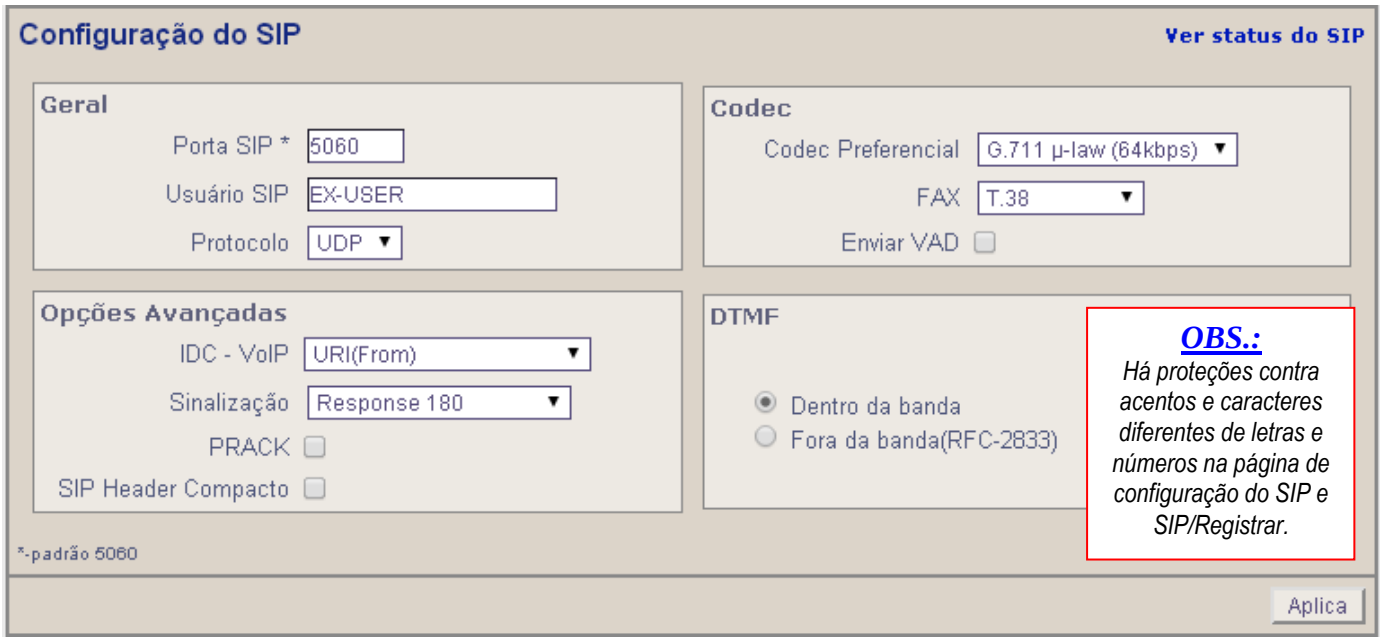
As ligações IP são feitas no VoIP usando o protocolo SIP (Session Initiation Protocol, RFC3261). Este serve para negociar os parâmetros da comunicação via rede, escolhendo endereço e compactação para o envio e recepção de áudio. Depois de estabelecida a chamada, os pacotes de áudio trafegam usando o protocolo RTP (Real-time Transport Protocol, RFC3550 e RFC3551).

O protocolo SIP oferece a opção de usar um servidor SIP (Registrar/Proxy), que funciona como uma central de endereços SIP, onde cada ponto tem um nome de usuário associado ao seu endereço real. Nesse caso todas as mensagens SIP para outros pontos registrados no servidor Registrar/Proxy serão encaminhadas para o servidor, que através de seu banco de dados de usuários registrados irá encaminhá-las para o endereço correto. Isso é usado pelas operadoras VoIP.

Quando uma chamada é negociada, o protocolo de sinalização usado (SIP) precisa passar para o outro ponto de comunicação o endereço para onde deve ser enviado o áudio. Esse endereço precisa ser acessível a partir do outro ponto de comunicação, caso contrário a conexão não terá áudio. Se a WAN do Gateway Digistar estiver conectada à Internet através de um NAPT, ou seja, tiver um endereço IP de uma rede interna não-roteável, o STUN deverá ser habilitado para que as ligações VoIP tenham áudio.

3.3.1. Configuração do SIP

3.3.1.1. Habilitar SIP (Configurações Gerais)



OBS.:
Estas configurações só se aplicam ao SIP Integrado, exceto a Porta SIP.

- **Habilitar SIP:** Habilita/Desabilita o protocolo SIP para chamadas VoIP.

Geral:

- Porta SIP: porta local onde serão recebidas as mensagens pertencentes ao protocolo SIP. A porta padrão é 5060.
- Usuário SIP: identificação enviada pelo Gateway Digistar nos pacotes SIP em ligações que não usem o cliente registrar, por exemplo, uma ligação para um número. IP.
- Protocolo: Protocolo de transporte utilizado para sinalização SIP. Os protocolos disponíveis são UDP e TCP. O mais usado é o UDP.

Codec:

- Codec Preferencial: compressão de áudio que terá preferência na negociação da chamada. Caso a outra ponta da chamada não suporte a codificação escolhida, outro codec será usado automaticamente.
  Codecs disponíveis: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps).

- Enviar VAD: Não envia pacotes ou envia pacotes menores quando detecta silêncio.

- FAX: Escolha do codec que será usado para a recepção de FAX via VoIP. Para que o T.38 funcione, o aparelho de FAX que irá receber deve estar configurado para recepção automática. Ao enviar um FAX via VoIP é o ponto que recebe o FAX que determina o protocolo a ser usado.
  Codecs disponíveis: G.711 e T.38.

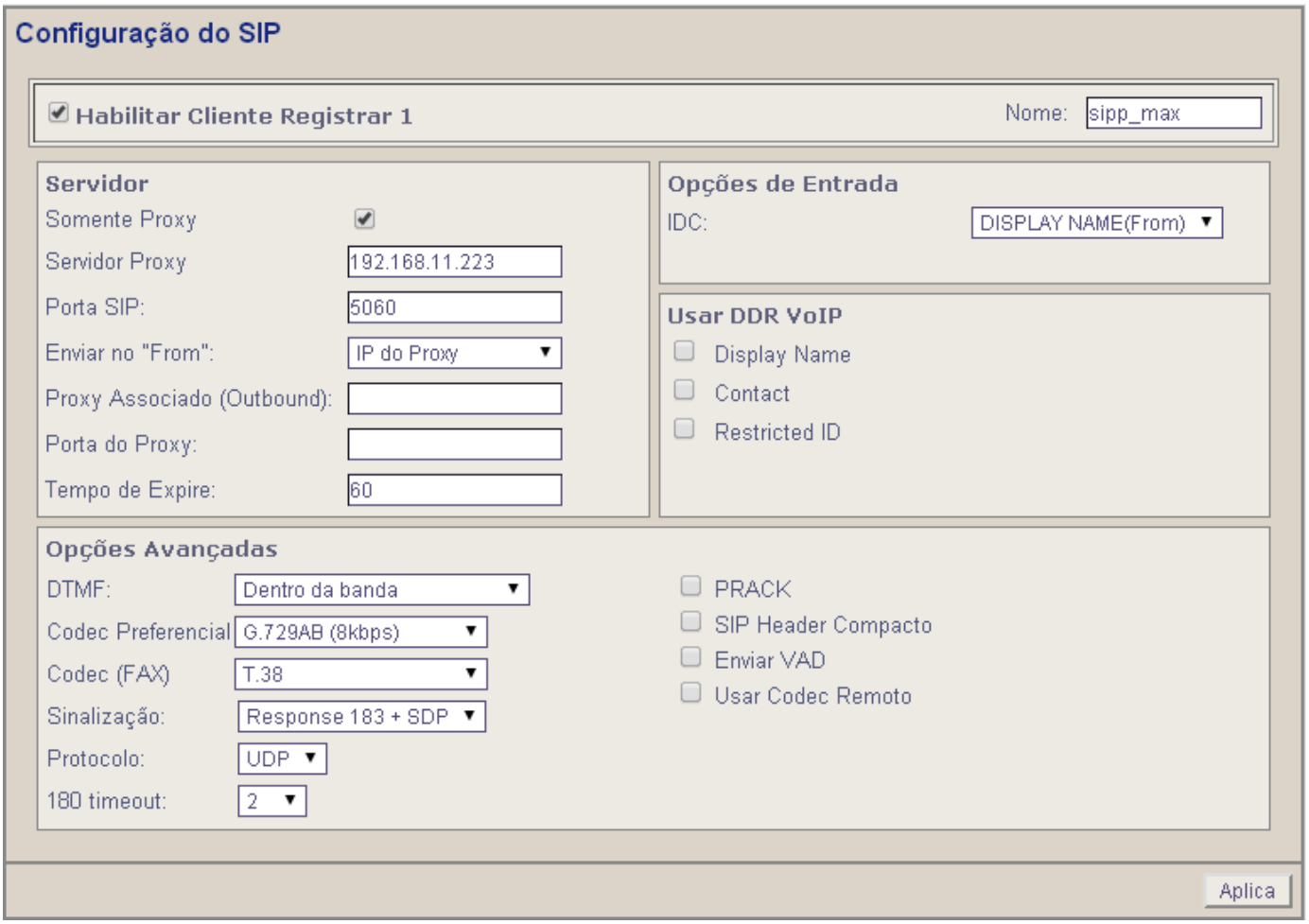
OBS.: *A funcionalidade T38 poderá não operar corretamente, pois depende das características de rede, tais como: jitter e atraso de rede, bem como da velocidade dos aparelhos de fax envolvidos na conexão.*

- **DTMF:** Método de transmissão de dígitos DTMF, pode ser dentro ou fora da banda. Quando estiver selecionado dentro da banda o DTMF é enviado com o áudio, podendo apresentar distorções que impossibilitam sua detecção pelo equipamento que irá recebê-lo.
No DTMF fora da banda é usada a norma RFC2833, onde o dígito é enviado em um pacote RTP.

- **Opções Avançadas:**
  - **IDC – VoIP:** Permite configurar qual campo do pacote SIP será utilizado para identificar a origem de ligações de entrada. São disponíveis os campos URI (From), que é o caso mais comum, DISPLAYNAME (From), que permite uma identificação mais amigável, porém é um campo não obrigatório, e URI (Contact), que comumente identifica o dispositivo de origem da ligação.
  - **Sinalização:** Envio do 180 sem SDP ou 180/183 com SDP e respectivo início de áudio. São respostas para ligações de entrada.
  - **SIP Header Compacto**: Envia as mensagens SIP com headers compactos (RFC 3261 e RFC 6262)
  - **PRACK:** Habilita a RFC 3262 (Reliable Provisional Responses).

3.3.1.2. Habilitar Servidores SIP

Configuração dos servidores SIP (Registrar/Proxy) que serão utilizados para realizar e receber as ligações VoIP. É possível configurar até cinco (5) servidores SIP.



- **Habilitar Servidor SIP:** Habilita/Desabilita a utilização do servidor VoIP configurado.

  - ***Nome:*** Identificação amigável da operadora. Este campo pode conter qualquer valor e não é utilizado para a realização das chamadas.

  - ***Somente Proxy:*** Esta opção desabilita o envio do pedido de registro para o servidor SIP. As chamadas são encaminhadas para o endereço do servidor SIP Registar/Proxy sem que a mensagem REGISTER seja enviada.

- ***Enviar no From*:** indica qual IP será usado na identificação do Access Gateway quando este originar uma chamada ao Servidor Proxy, sendo as opções disponíveis: o IP Local do Access Gateway ou o IP do Proxy. Para efetuar essa configuração a operadora deve ser consultada quanto à identificação da origem das chamadas.

- ***Servidor Registrar/Proxy:*** endereço IP do servidor Registrar/Proxy.
- ***Porta SIP:*** porta do servidor registrar para a qual serão direcionadas as mensagens do protocolo SIP enviadas pelo Gateway Digistar. A porta padrão é 5060.
- ***Tempo de Expire*:** duração dos registros em segundos. Após esse tempo, caso não tenha sido renovados, os registros são apagados do servidor.
- ***Proxy Associado (Outbound):*** endereço do servidor que irá redirecionar os pacotes para o servidor Registrar/Proxy.
- ***Porta Proxy:*** porta do Proxy Associado (*Outbound*) para a qual serão direcionadas as mensagens SIP. A porta padrão é a 5060.

- **Opções de Entrada:**

- **IDC:** permite configurar qual campo da mensagem INVITE do SIP será utilizado como o identificador da chamada (IDC) nas ligações de entrada efetuadas por esse Servidor ao Access Gateway.
  São disponíveis os campos User(From), que é o caso mais comum, DISPLAYNAME(From), que permite uma identificação mais amigável, porém é um campo não obrigatório, e URI(Contact), que comumente identifica o dispositivo de origem da ligação. O valor que vier no campo selecionado será utilizado nas regras de redirecionamento do VoIP para o TDM nas ligações provindas do domínio desse Servidor SIP. (ver seção: Redirecionamento).
  Obs.: caso for selecionada a opção DISPLAYNAME (From) e o INVITE chegar com esse campo vazio, será utilizado o valor do campo User (From).

- **Usar DDR VoIP:**
  - Campos Display Name, Contact e Restricted ID: Opção utilizada em ligações de saída por operadora VoIP. Permite substituir o valor programado nos campos display name, contact e restricted ID pela identificação de chamada recebida da origem da ligação. Esta configuração tem precedência sobre os valores configurados nos campos de conta. Em casos onde a identificação de chamada da origem for desconhecida são enviados os valores configurados nos campos de operadora.

- **Opções Avançadas:**

- **DTMF:** Método de transmissão de dígitos DTMF, pode ser dentro ou fora da banda. Quando estiver selecionado dentro da banda o DTMF é enviado com o áudio, podendo apresentar distorções que impossibilitam sua detecção pelo equipamento que irá recebê-lo.
  No DTMF fora da banda é usada a norma RFC2833, onde o dígito é enviado em um pacote RTP.

- **Codec Preferencial:** compressão de áudio que terá preferência na negociação da chamada. Caso a outra ponta da chamada não suporte a codificação escolhida, outro codec será usado automaticamente.
  - Codecs disponíveis: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps).

- **Codec (FAX):** Escolha do codec que será usado para a recepção de FAX via VoIP. Para que o T.38 funcione, o aparelho de FAX que irá receber deve estar configurado para recepção automática. Ao enviar um FAX via VoIP é o ponto que recebe o FAX que determina o protocolo a ser usado. Codecs disponíveis: G.711 e T.38.

- **Sinalização:** Envio do 180 sem SDP ou 180/183 com SDP e respectivo início de áudio. São respostas para ligações de entrada.

- **Protocolo:** Define o protocolo de transporte da sinalização SIP desse servidor. Atualmente tem-se disponível o protocolo UDP.

- **180 Timeout:** Em alguns casos de ligações recebidas via uma operadora VoIP, o tratamento dessa recepção pode demorar alguns instantes, dependendo para onde a ligação será encaminhada. Esse comportamento atrasa o envio da mensagem SIP 180 (RINGING) para a operadora VoIP, consequentemente atrasando a audição do tom de chamando para quem está efetuando a ligação. Esta configuração permite que seja ajustado um intervalo de espera durante o tratamento da ligação recebida para que o Gateway Digistar envie espontaneamente a mensagem 180 (RINGING) à operadora VoIP. Esse intervalo pode variar entre 0 e 30 segundos.

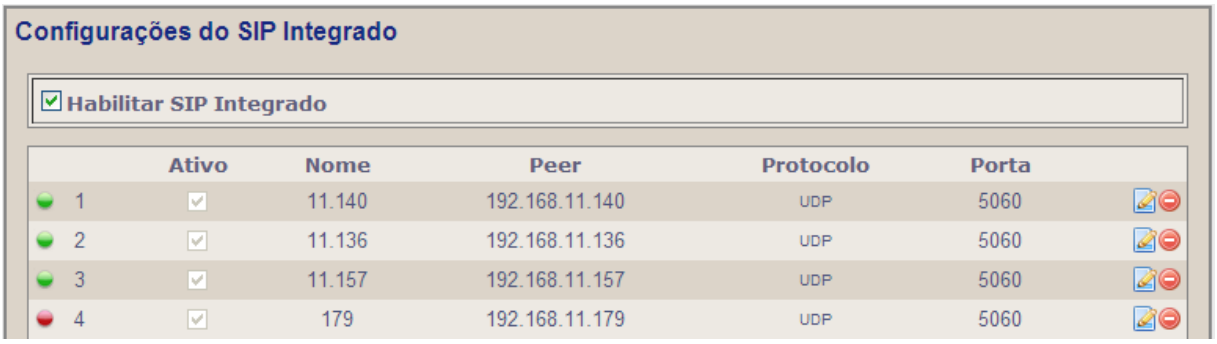
- **PRACK:** Habilita a RFC 3262 (Reliable Provisional Responses).

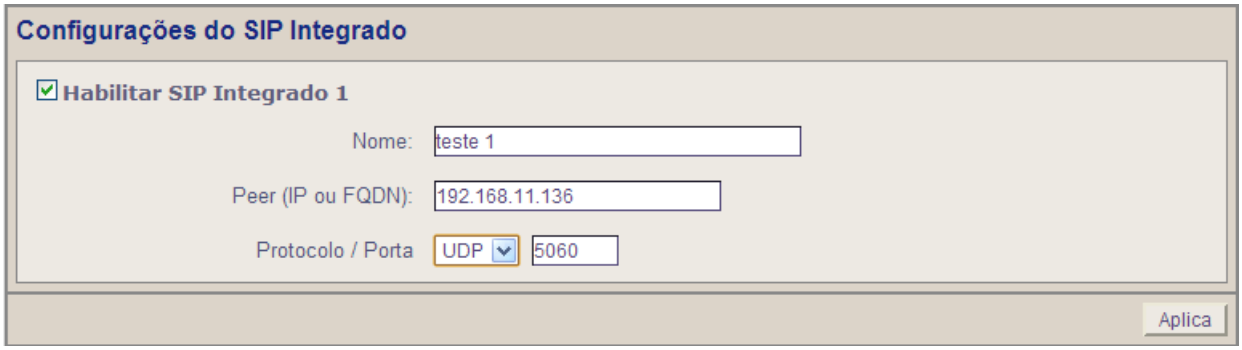
- **SIP Header Compacto**: Envia as mensagens SIP com headers compactos (RFC 3261 e RFC 6262)

- **Enviar VAD:** Não envia pacotes ou envia pacotes menores quando detecta silêncio**.**

- **Usar Codec Remoto:** Nesta opção, durante uma negociação iniciada pelo servidor registrar, o primeiro codec ofertado pelo servidor terá prioridade sobre o codec preferencial configurado.

3.3.2. Configurações SIP Integrado





Objetivo

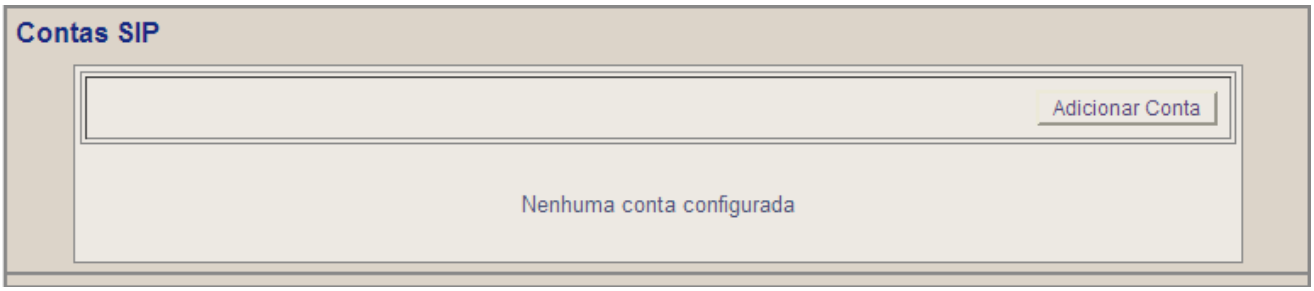
Funcionalidade que permite interligar equipamentos distintos (pontos) através da interface IP**.**

Premissas

- Cada ponto será ***independente dos demais***. A configuração de cada ponto será própria, com programações específicas.
- O número de pontos remotos máximo é 64.

3.3.2.1. Configurar Contas SIP

Para que seja possível realizar as ligações VoIP é necessário cadastrar as contas SIP e associá-las a um dos servidores SIP cadastrados. É possível cadastrar até 1.000 contas.



- ***Usuário****:* identificação usada para o registro no servidor e nas chamadas VoIP que utilizam o servidor SIP Registrar/Proxy. Este é o campo a ser analisado pela operadora VoIP para identificar o usuário de destino.

- ***Senha****:* usada para a autenticação no servidor SIP Registrar/Proxy.

- ***Display Name****:* campo de texto opcional para identificação do usuário que utiliza a conta.

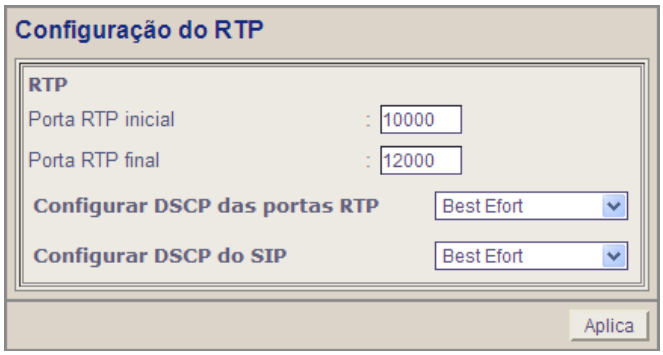
- ***Contact***: ***Login***: usuário usado para autenticar a conta no Servidor SIP. Só é preenchido se o usuário de autenticação for diferente da identificação de registro da conta. Se não for preenchido o Gateway Digistar usa o campo *Usuário* para autenticar a conta.

- ***Restricted ID:*** (texto – identificação adicional): substitui o usuário como identificador. Caso em que o valor "*anonymous"* é enviado para a operadora VoIP, no campo de usuário.

- ***Servidor***: número do servidor SIP Registrar/Proxy onde a conta SIP irá se registrar e encaminhar as ligações.

- ***Permitir ligações simultâneas***: permite ou bloqueia que uma conta SIP, mesmo ocupada, possa fazer outras ligações. Isso evita que o Gateway Digistar fique enviando ligações não permitidas pela operadora, diminuindo o tempo de resposta ao usuário e as mensagens na rede. (Obs.: essa opção não vale para as ligações de entrada, VoIP para TDM, a quais sempre são aceitas, mesmo que a conta SIP esteja ocupada).

3.3.2.2. Configuração de RTP


Configuração do RTP
RTP
Porta RTP inicial : 10000
Porta RTP final : 12000
Configurar DSCP das portas RTP Best Efort
Configurar DSCP do SIP Best Efort
Aplica

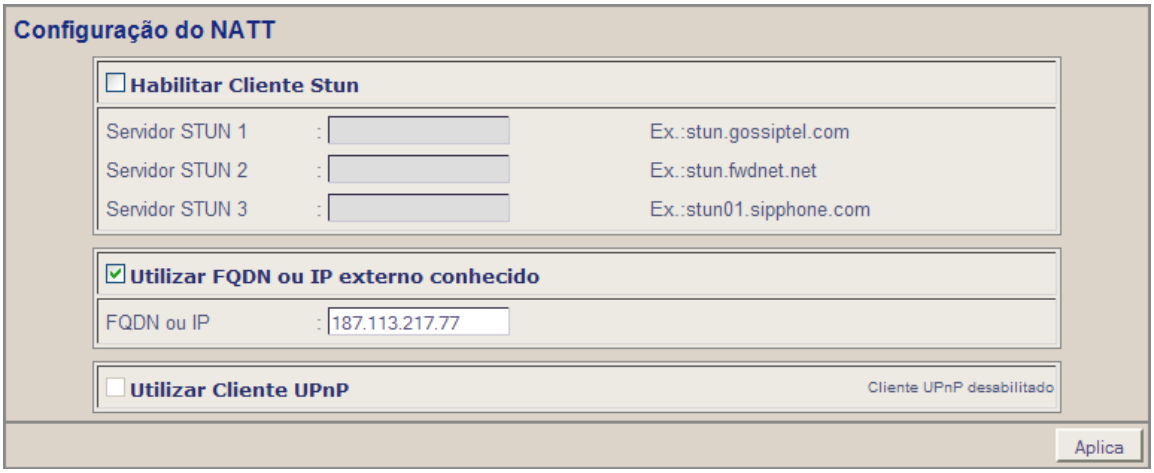
- **RTP:** Permite especificar o intervalo de portas que será usado para a recepção do áudio. Somente são usadas as portas pares do intervalo.
    - Porta RTP inicial: primeira porta do intervalo de portas disponíveis para RTP.
    - Porta RTP final: última porta do intervalo de portas disponíveis para RTP.

- **Configurar DSCP das portas RTP**: Permite configurar a prioridade dos pacotes de áudio (RTP) do VoIP (Serviços diferenciados, DiffServ).

- **Configurar DSCP SIP:** Permite configurar a prioridade dos pacotes do protocolo SIP.

A taxa de amostragem padrão é de 20 ms para o G711 e G729. O cancelamento de eco é de até 128ms.

3.3.3. Configuração do NATT



- **Habilitar Cliente Stun:** Simple Traversal of UDP through NAT (RFC3489). O STUN deve ser ativado somente se o Gateway Digistar estiver conectado à Internet através de um NAPT.

    - Servidor STUN: endereço do servidor STUN na Internet. Podem ser preenchidos até três endereços para o caso de algum deles não estar funcionando.

- **Utilizar FQDN ou IP externo conhecido:** Caso seja conhecido o IP externo ou o FQDN (nome do domínio, por exemplo, www.digistar.com.br) e o Gateway Digistar estiver conectado à Internet através de um NAPT.

- **Utilizar cliente UPNP** Para os casos em que o Gateway Digistar estiver atrás de um NAPT que tenha um Servidor UPNP rodando. Para utilizar é necessário habilitar o campo cliente UPnP no campo serviços/ UPNP.

OBS.: *Esta opção só pode ser habilitada quando o firewall estiver desabilitado*

3.3.4. Configurações de QoS

Introdução:

Originalmente a Internet não foi desenvolvida para suportar tráfegos de tempo real, tal como VoIP. Com o avanço desses tipos de aplicações necessitou-se elaborar mecanismos para a garantia de qualidade. Assim, surgiu o conceito de QoS, que é a sigla em inglês para Qualidade de Serviço. Basicamente, nessa técnica são aplicadas políticas para assegurar um tratamento diferenciado dependendo das necessidades de cada tipo de aplicação.

QoS em VoIP

A qualidade das ligações VoIP está relacionada com fatores como: o atraso total desde a captura da voz até a sua reprodução no usuário final; a variação do atraso (ou *jitter*), o qual provoca uma sensação de desconforto nas conversações; o descarte de pacotes, que ocasiona a interrupção da voz; e também o *codec* utilizado, que pode codificar e comprimir a voz com maior ou menor impacto no áudio original.

Assim, para garantir premissas de qualidade nas ligações devem-se aplicar mecanismos que diminuam o tempo em que os pacotes ficam retidos nos roteadores, que possibilitem a cadência dos fluxos e que diminuam a probabilidade de perdas dos pacotes.

Para isso, são utilizadas técnicas de QoS, onde os fluxos são classificados e tratados com maior ou menor prioridade dependendo do tipo de aplicação. Nesses métodos se abrage também a reserva de faixas da banda conforme as necessidades para o encaminhamento dos pacotes.

A seguir é apresentada uma visão de métodos de QoS e como é possível configurá-lo no Gateway Digistar.

Classificação dos Pacotes

Historicamente se utilizava como política de QoS o conceito de Intserv (Serviços Integrados) que é um modelo baseado em reserva de recursos, onde a máquina final envia para toda a rede sua necessidade de banda. Atualmente um número muito pequeno de roteadores no mercado utiliza o Intserv, pois esse protocolo só funciona se todos os roteadores estiverem configurados corretamente.

A técnica evolutiva consiste no conceito de "Serviços Diferenciados" ou DiffServ, em que os pacotes são marcados de acordo com classes de serviços pré-determinadas e desse modo são tratados, diferencialmente, nos roteadores que suportam esse protocolo. Nessa abordagem cada roteador tratará as diferentes classes conforme as configurações nele previamente determinadas, não necessitando a interação com outros componentes. Assim, caso algum roteador não suporte esse protocolo, o tratamento privilegiado ainda poderá ser realizado nos demais roteadores.

Com esse mecanismo pode-se, como exemplo, marcar os pacotes de voz com maior prioridade e assim privilegiá-los nas filas dos roteadores com suporte ao DiffSev, diminuindo a latência, o *jitter* e o descarte dos pacotes no caso de congestionamento.

A marcação dos pacotes no "Serviço Diferenciado" é realizada por meio do campo DSCP (*Differenciated Services Code Point)* do cabeçalho IP *(Internet Protocol),* o qual substitui a utilização do campo TOS *(Type of Service).* Podem-se marcar os pacotes com as seguintes classes pré-definidas:

- **Best Efort - BE: (Melhor Esforço):** Sem alteração no campo de Serviços Diferenciados (RFC – 2474);

- **Class Selector (Seleção de Classe):** Semelhante às categorias de precedência utilizadas no campo do ToS.
Podem ser definidas como IP-Precedence 1 a IP-Precedence 7 (RFC – 2474);

- **Assured Forwarding-AF (Encaminhamento Garantido):** A marca AF é a forma intermediária de marcação entre o Class Selector e o Expedicted Forwarding. Ela pode ser dividida em 4 classes de precedência e 3 níveis de probabilidade de pacotes (alto, médio, baixo). (RFC – 2597);

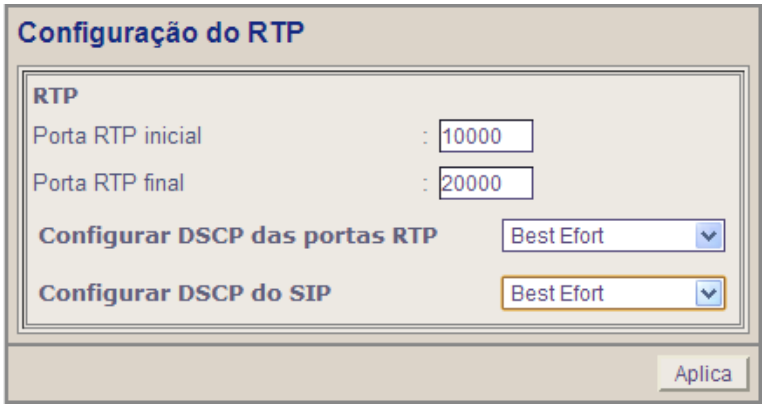
- **Expedicted Forwarding-EF (Encaminhamento de expedição):** A marca EF é a forma de garantir o menor atraso, menor perda, menor variação de atraso e maior qualidade, utilizado principalmente para aplicações VoIP(RFC -2598).

Observa-se que a marcação dos pacotes não garante que eles serão tratados com os privilégios definidos, uma vez que é necessário que o roteador envolvido tenha suporte ao DiffServ.O Gateway Digistar apresenta um suporte completo ao DiffServ, onde além de realizar a marcação também implementam políticas para tratar os pacotes recebidos conforme a sua classe. Os pacotes com maior prioridade são tratados mais rapidamente, sendo encaminhados à rede antes dos pacotes com menor prioridade, diminuindo assim o tempo de espera nas filas do Gateway Digistar.

A seguir são apresentados os modos de classificação dos pacotes no Gateway Digistar. Pode-se realizar a marcação classificando todos os pacotes RTP para uma determinada classe DiffServ.Também é possível definir uma classe para uma máquina ou um intervalo específico de máquinas e serviços.

Classificando todos os pacotes RTP (VoIP):

Na página de configuração do RTP é possível mudar o parâmetro DSCP dos fluxos RTP e SIP.



Com isso, pode-se privilegiar o tráfego de voz na saída do Gateway Digistar e nos roteadores, no caminho até o destino final, que apresentem suporte ao DiffServ.

Classificando tráfegos específicos

Na página de configuração do QoS pode-se determinar a marcação DSCP para outros tipos de tráfegos (TCP, UDP, GRE ou TODOS), onde pode-se ainda definir computadores específicos, ou um intervalo de computadores, uma rede e até portas específicas.

Como exemplo dessa classificação poderia-se alterar o campo DSCP do fluxo de voz dentro do intervalo de portas entre 10000 a 12000 de um telefone IP com endereço 192.168.10.32 para a classe de maior prioridade (EF Class). Assim, esse telefone específico teria um maior privilégio em relação aos demais, caso eles não fossem marcados ou apresentassem uma classe com menor prioridade.

Reserva de Banda:

Outra maneira de garantir premissas de QoS para as ligações consiste em reservar a banda. Aplicações VoIP utilizam, consideravelmente, tanto os canais de download quanto os de upload para a transmissão dos pacotes de voz. Desse modo, em cenários onde a voz é transmitida no mesmo link que fluxos de dados, existirá uma concorrência pela ocupação da banda, em que, nos casos de congestionamento, poderá ocasionar o atraso ou até o descarte dos pacotes de voz. Desse modo, uma maneira de minimizar esse problema consiste em definir regras de QoS para reservar uma percentagem da banda para uso dos tráfegos de voz.

No Gateway Digistar pode-se reservar a banda de duas maneiras: limitando o tráfego total de TCP na banda ou determinando a reserva especificamente para uma máquina ou um intervalo determinado de máquinas e serviços. A seguir serão explicados os modos de reservar a banda no Gateway Digistar.

Configurações de QoS
Habilitar o suporte a QoS
Direção Velocidade (Vazão)
Upload 160 kbit/s
Download 320 kbit/s
Limite de banda TCP na LAN: 45 %
IP Máscara Faixa de portas Protocolo % da banda Alterar DSCP
192.168.10.50 255.255.255.0 8080 TCP 20 Não alterar
192.168.10.32 255.255.255.0 10000-12000 UDP EF Class
TCP Não alterar
TCP Não alterar
Aplicar

Reservando a banda para todas as ligações VoIP

Utilizando-se do campo “Limite de banda TCP na LAN” é possível restringir a um valor percentual a ocupação da banda pelo tráfego TCP (percentual do valor preenchido em “Upload” e “Download”), reservando o restante para as ligações VoIP. Essa reserva é realizada de modo dinâmico, ou seja, caso a percentagem de banda reservada para as ligações VoIP não esteja

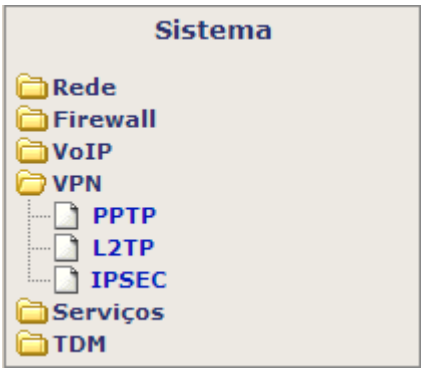
totalmente ocupada, o tráfego TCP poderá extrapolar o limite definido, não prejudicando as ligações ativas e ocupando a faixa de banda ociosa. Observa-se que esses controles também valem para o tráfego VoIP, ou seja, os tráfegos das ligações só poderão ocupar a banda do tráfego TCP quando esse não estiver utilizando o percentual para ele destinado. Essa política permite garantir a qualidade das ligações, utilizando a banda de um modo eficiente e justo aos tráfegos envolvidos.
Para determinação da reserva deve-se definir na página de configuração o limite de ocupação máximo do tráfego TCP quando existem ligações ativas (Limite de banda TCP na LAN) e os parâmetros de velocidade do uplink (Upload) e velocidade do downlink (Download).

Reservando a banda para tráfegos específicos

Tal como a marcação DSCP pode-se reservar a banda para máquinas e serviços específicos. Para isso, utiliza-se a mesma maneira de configuração específica de QoS, ou seja, pode-se determinar um computador ou intervalo de computadores, definir as portas associadas e o tipo de tráfego (TCP, UDP, GRE ou TODOS). Com isso, pode-se, por exemplo, reservar 20% do total da banda para um servidor WEB no endereço 192.168.10.50.

Nota-se que na configuração específica de QOS é possível reservar a banda e marcar (classificar) os pacotes ao mesmo tempo.

3.4. VPN



VPN (Redes Virtuais Privadas) é uma extensão das redes privadas, pois fazem a união de redes privadas que estão separadas fisicamente como uma ligação ponto a ponto. Usualmente a união destas redes é feita através de um meio público, como a Internet, onde o uso de criptografia faz-se necessário.

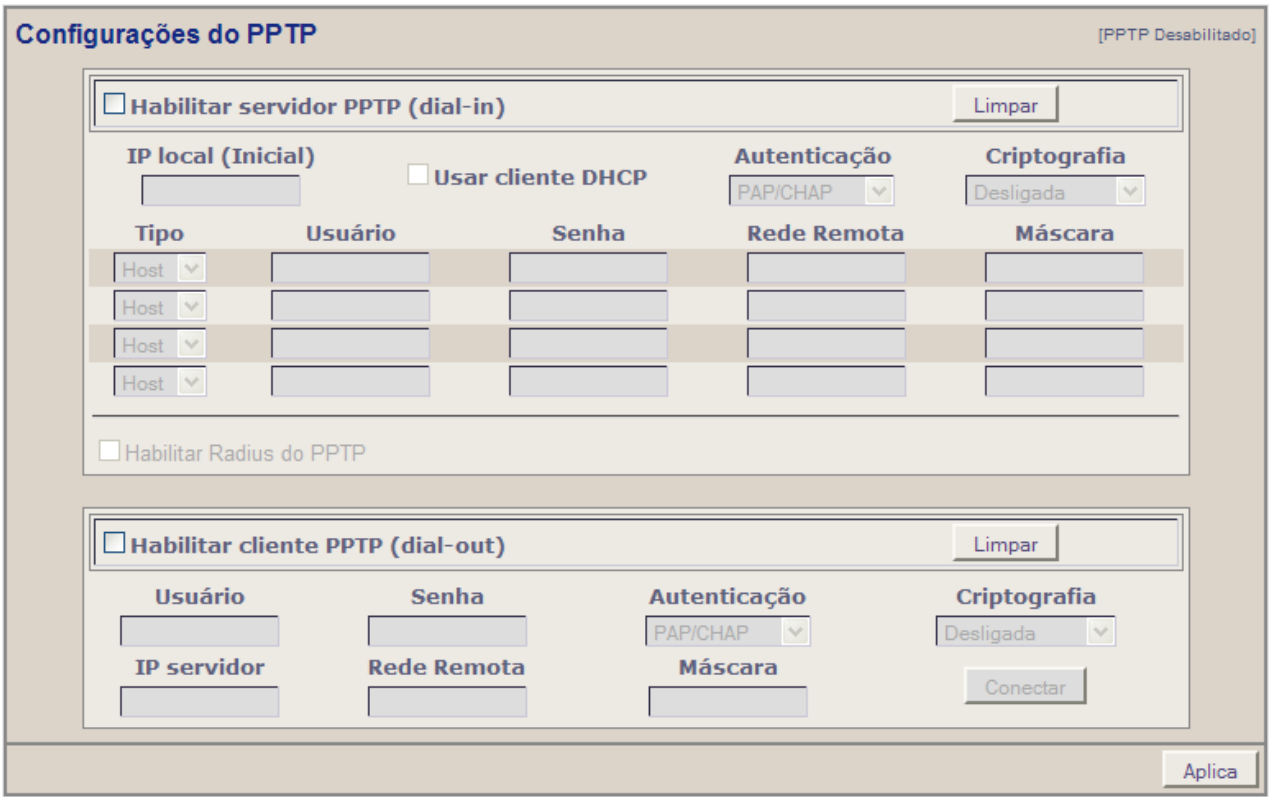
Podem ser divididas em dois grandes grupos:

- Conexão de discagem remota, também chamada de Cliente-LAN. Usada para que um usuário remoto, por exemplo, um usuário em um hotel, possa acessar a rede privada de maneira segura.

- Conexão entre redes, também chamada de LAN-to-LAN ou GW-to-GW. Usada para que se estabeleça uma conexão segura entre redes privadas. É usada muito entre clientes - fornecedores e matriz - filiais.

O Gateway Digistar tem os três protocolos mais comuns para estabelecer até 4 VPNs. Os protocolos são PPTP, L2TP e o IPSEC. Todos os protocolos podem ser utilizados para fazer conexões do tipo LAN-to-LAN, Para as conexões do tipo Cliente-LAN são mais utilizados os protocolos PPTP e L2TP.

3.4.1. Configurações do PPTP



A sigla PPTP significa protocolo de túnel ponto a ponto. É um mecanismo de encapsulamento para transferir quadros PPP, onde é possível utilizá-lo para fazer criptografia e autenticação de usuários.
O PPTP utiliza a porta TCP 1723 para controle e utiliza encapsulamento com o protocolo GRE (Generic Routing Encapsulation) para a transmissão de dados. (RFC 2637)

Como servidor permite:

- **Sem RADIUS e sem DHCP:** Permite até 4 conexões VPN. Configura-se um IP inicial fora do range do servidor DHCP e cada usuário que se conectar irá ganhar um IP entre o IP inicial e o IP inicial + 3. Assim se eu tiver 4 usuários User1, User2, User3 e User4, com o IP inicial 192.168.10.100, quando o usuário User1 se conectar irá ganhar o IP 192.168.10.100, quando o usuário User2 se conectar ganhará o IP 192.168.10.101, e assim até o User4 com o IP 192.168.10.103. Para que não haja conflito de IPs, é necessário usar o servidor DHCP (tela Rede e DHCP) com os limites de IPs que não colidam com os endereços do PPTP. Assim, no nosso exemplo, deveria ser configurado o servidor DHCP com IP final até 192.168.10.99 ou com o IP inicial a partir de 192.168.10.104.

- **Com RADIUS e sem DHCP:** Permite até 4 conexões. Semelhante a forma acima, com a diferença que os usuários e senhas devem ser colocados no servidor RADIUS, para o mesmo fazer a autenticação. Para habilitar o RADIUS: Configurações de SNMP/Syslog e Radius.

- **Sem RADIUS e com DHCP:** Permite múltiplas conexões com até 4 usuários distintos. Não há mais configuração do IP inicial e os IP são fornecidos para os usuários através do servidor DHCP da rede. É a maneira mais fácil de estabelecer uma conexão PPTP. Desta forma, a cada conexão é fornecido um IP diferente, mesmo sendo o mesmo usuário. Assim, por exemplo, podemos criar um usuário "*vendedores"* e um usuário "*fornecedores"*. Todos os vendedores podem acessar a rede privada usando o mesmo login "*vendedores",* assim como todos os fornecedores o login "*fornecedores"*.

- **Com RADIUS e com DHCP:** Permite múltiplas conexões com até 4 usuários distintos. Irá usar o servidor DHCP para fornecer IPs e irá fazer autenticação usando o servidor RADIUS.

Existem três formas de autenticação:

- PAP – (Protocolo de Autenticação por Senha) – É a forma de autenticação que envia o usuário e a senha em aberto na rede, sem nenhuma criptografia. É a maneira menos segura de autenticação.

- CHAP – (Protocolo de Autenticação de Desafio de Resposta) – Utiliza protocolo de codificação Message Digest 5 (MD5) de um só sentido. A senha é enviada de forma codificada.

- MS-CHAPv2 (Protocolo de Autenticação de Desafio de Resposta da Microsoft versão 2) – Utiliza protocolo de codificação Message Digest 4 (MD4) em ambos os sentidos ou autenticação mútua.

  Para a criptografia dos dados é possível usar o protocolo MPPE (Encriptação Ponto a Ponto da Microsoft) que cria chaves criptográficas diferentes para cada sentido de transmissão, além de trocar a chave periodicamente. As chaves podem ser de 40 ou 128bits RSA RC-4. Para usar a criptografia é preciso selecionar a forma de autenticação para MS-CHAPv2. Existe também um campo para usar criptografia opcional, ou seja, cria a conexão mesmo sem criptografia. A maneira mais segura é usar autenticação por MS-CHAPv2 e criptografia de 128 bits.

Com o PPTP é possível criar conexões do tipo Cliente-LAN ou LAN-to-LAN. A forma de uso é definida pelo campo TIPO. Se o campo estiver como *rede* irá se estabelecer uma conexão do tipo LAN-to-LAN, assim como se estiver como *host* irá se estabelecer uma conexão do tipo Cliente-LAN. Para conexão do tipo LAN-to-LAN é necessário informar o número de rede remota e a máscara da rede remota. Vale lembrar que é necessário que as redes privadas das máquinas sejam diferentes para que o túnel LAN-to-LAN se estabeleça.

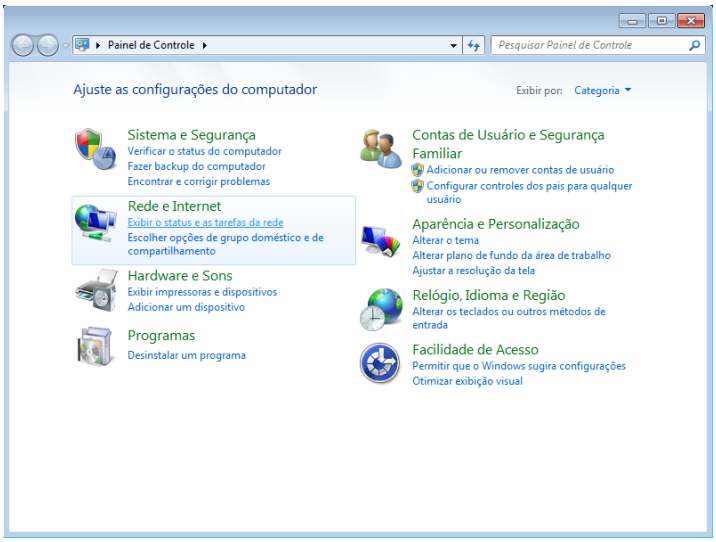
O Gateway Digistar pode funcionar como cliente PPTP, neste caso ele irá fazer a discagem para outra máquina (dial-out). Basta entrar com as configurações, aplicá-las e clicar no botão CONECTAR. O Gateway Digistar também pode atuar como servidor PPTP.

Para ver quais os túneis que estão ativos no momento, verifique na opção “Ver tabela de túneis PPTP”.

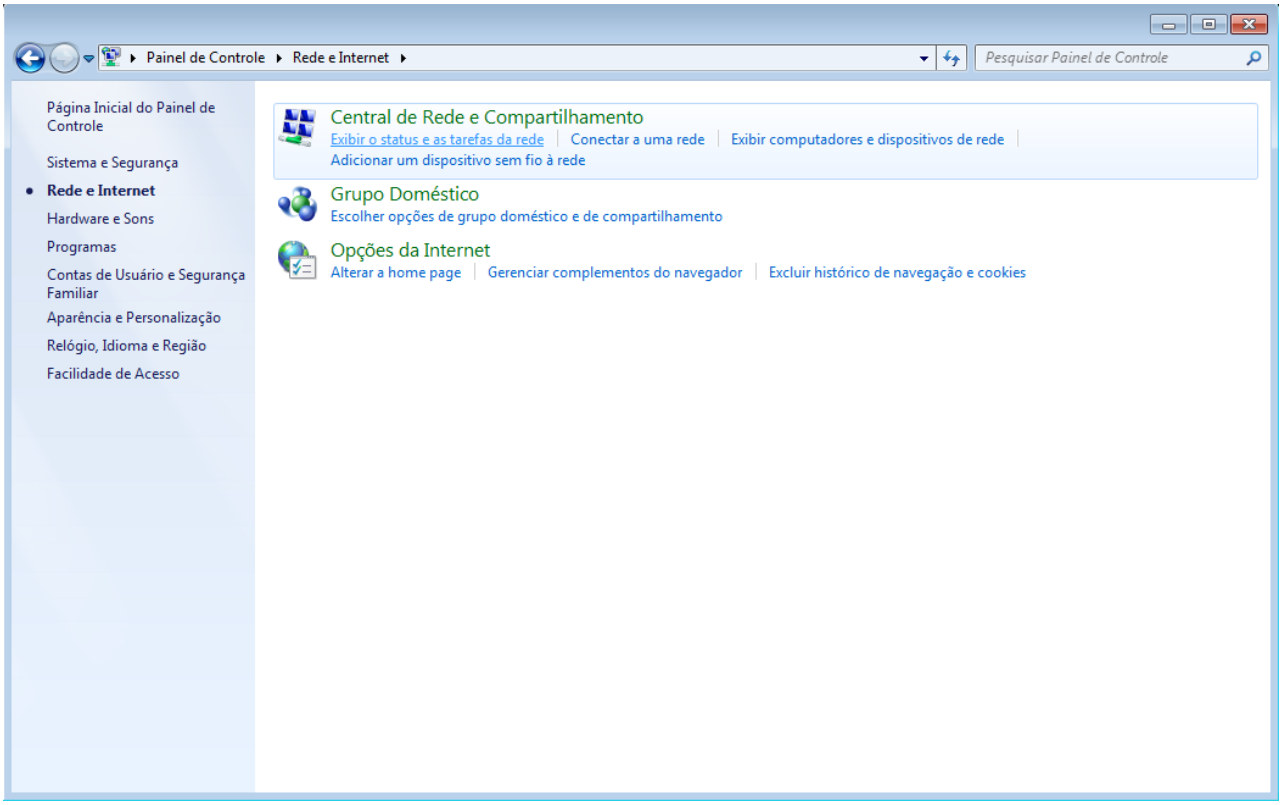
Quanto à compactação, o servidor PPTP do Gateway Digistar aceita o protocolo MPPC, ou Protocolo de Compactação Ponto a Ponto da Microsoft. O MPPC é definido pela RFC 2118 e utiliza compressão dos pacotes PPP, utilizando algoritmo baseado em LZ (também chamado de Lempel-Ziv) com buffer histórico de janela deslizante.

Os passos para fazer o túnel em ambiente Windows 7 são:

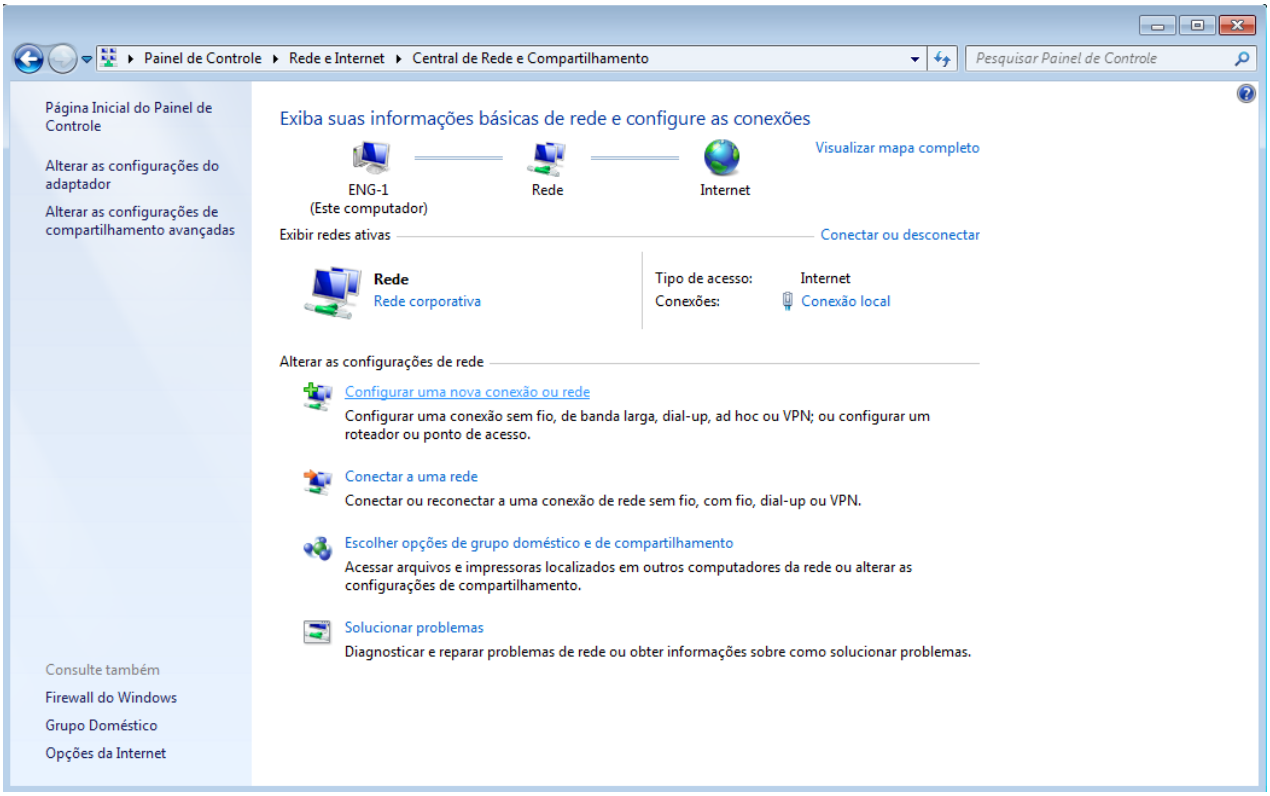
1 - Vá em "Painel de controle" e clique em "Rede e Internet"


Painel de Controle
Pesquisar Painel de Controle
Ajuste as configurações do computador
Exibir por: Categoria
Sistema e Segurança
Verificar o status do computador
Fazer backup do computador
Encontrar e corrigir problemas
Rede e Internet
Exibir o status e as tarefas da rede
Escolher opções de grupo doméstico e de compartilhamento
Hardware e Sons
Exibir impressoras e dispositivos
Adicionar um dispositivo
Programas
Desinstalar um programa
Contas de Usuário e Segurança Familiar
Adicionar ou remover contas de usuário
Configurar controles dos pais para qualquer usuário
Aparência e Personalização
Alterar o tema
Alterar plano de fundo da área de trabalho
Ajustar a resolução da tela
Relógio, Idioma e Região
Alterar os teclados ou outros métodos de entrada
Facilidade de Acesso
Permitir que o Windows sugira configurações
Otimizar exibição visual

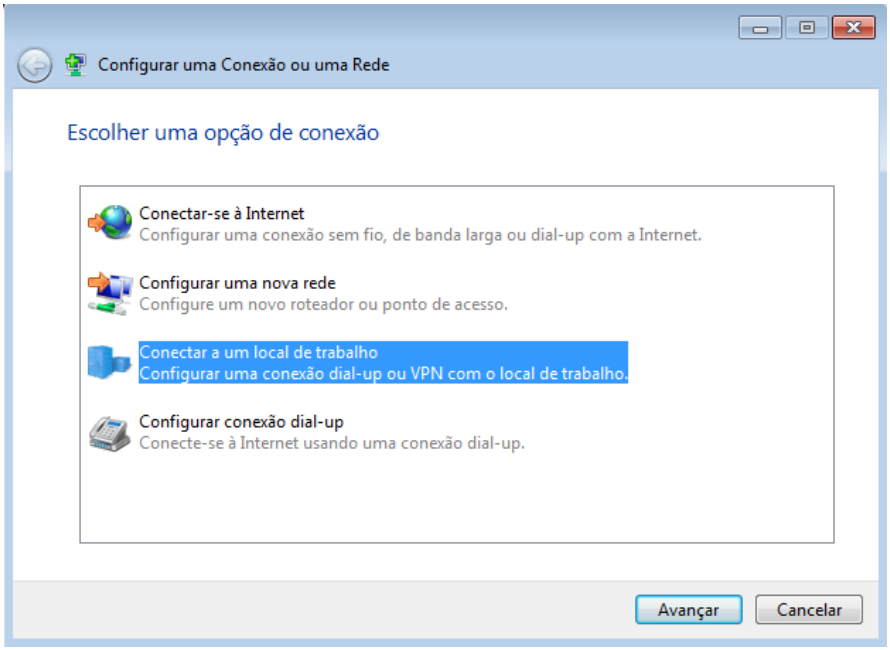
2 - Clique em "Exibir o status e as tarefas da Rede"


Painel de Controle
Rede e Internet
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Sistema e Segurança
Rede e Internet
Hardware e Sons
Programas
Contas de Usuário e Segurança Familiar
Aparência e Personalização
Relógio, Idioma e Região
Facilidade de Acesso
Central de Rede e Compartilhamento
Exibir o status e as tarefas da rede
Conectar a uma rede
Exibir computadores e dispositivos de rede
Adicionar um dispositivo sem fio à rede
Grupo Doméstico
Escolher opções de grupo doméstico e de compartilhamento
Opções da Internet
Alterar a home page
Gerenciar complementos do navegador
Excluir histórico de navegação e cookies

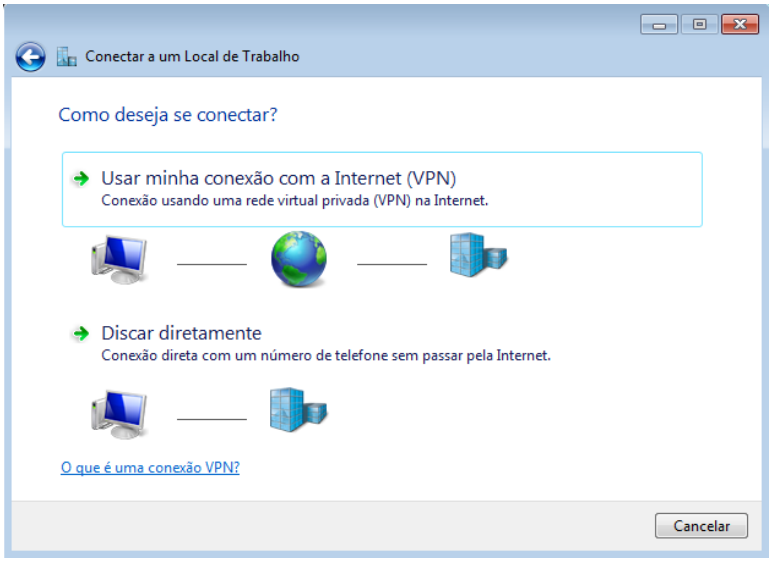
3 - Clique em "Configurar uma nova conexão ou rede"


Painel de Controle ▸ Rede e Internet ▸ Central de Rede e Compartilhamento
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Alterar as configurações do adaptador
Alterar as configurações de compartilhamento avançadas
Exiba suas informações básicas de rede e configure as conexões
Visualizar mapa completo
ENG-1
(Este computador)
Rede
Internet
Exibir redes ativas
Conectar ou desconectar
Rede
Rede corporativa
Tipo de acesso: Internet
Conexões: Conexão local
Alterar as configurações de rede
Configurar uma nova conexão ou rede
Configurar uma conexão sem fio, de banda larga, dial-up, ad hoc ou VPN; ou configurar um roteador ou ponto de acesso.
Conectar a uma rede
Conectar ou reconectar a uma conexão de rede sem fio, com fio, dial-up ou VPN.
Escolher opções de grupo doméstico e de compartilhamento
Acessar arquivos e impressoras localizados em outros computadores da rede ou alterar as configurações de compartilhamento.
Solucionar problemas
Diagnosticar e reparar problemas de rede ou obter informações sobre como solucionar problemas.
Consulte também
Firewall do Windows
Grupo Doméstico
Opções da Internet

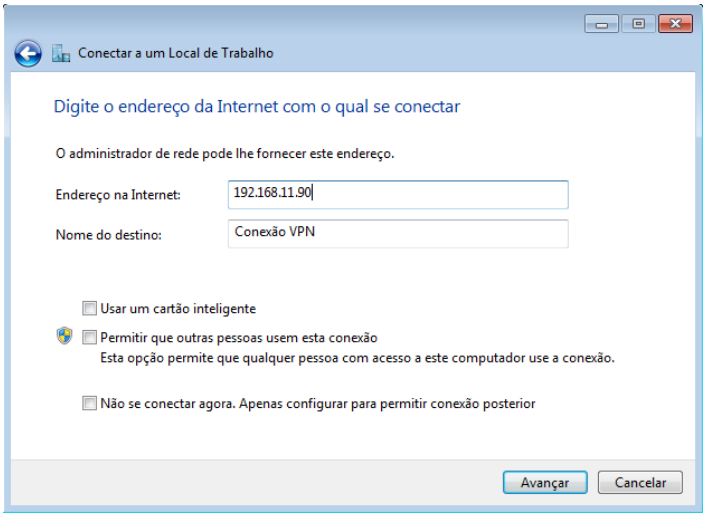
4 - Clique em "Conectar a um local de trabalho" e depois em "avançar"


Configurar uma Conexão ou uma Rede
Escolher uma opção de conexão
Conectar-se à Internet
Configurar uma conexão sem fio, de banda larga ou dial-up com a Internet.
Configurar uma nova rede
Configure um novo roteador ou ponto de acesso.
Conectar a um local de trabalho
Configurar uma conexão dial-up ou VPN com o local de trabalho.
Configurar conexão dial-up
Conecte-se à Internet usando uma conexão dial-up.
Avançar
Cancelar

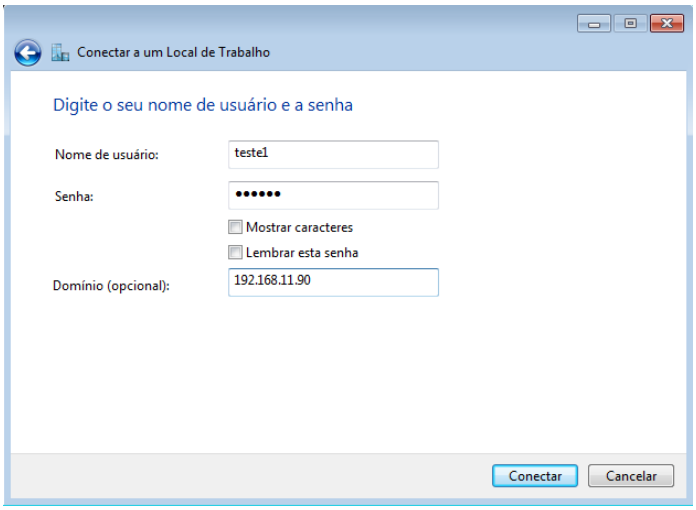
5 - Clique em "Usar minha conexão com a internet (VPN)"


Conectar a um Local de Trabalho
Como deseja se conectar?
Usar minha conexão com a Internet (VPN)
Conexão usando uma rede virtual privada (VPN) na Internet.
Discar diretamente
Conexão direta com um número de telefone sem passar pela Internet.
O que é uma conexão VPN?
Cancelar

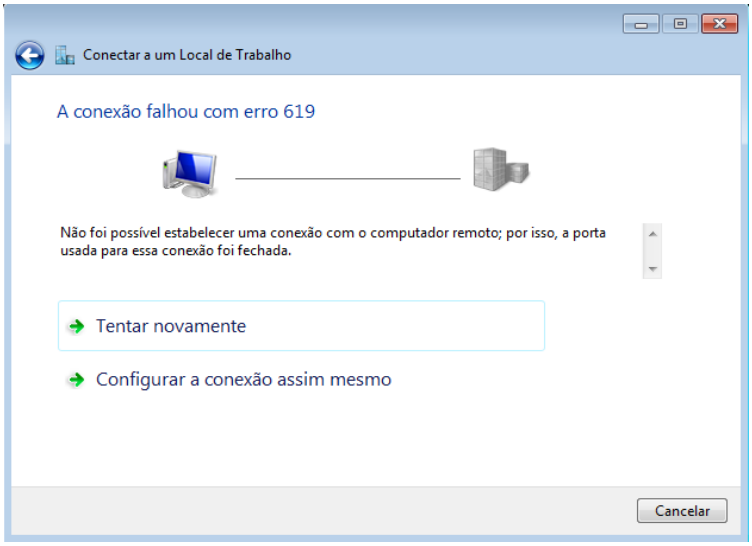
6 - Configure o IP onde será conectada a VPN e o nome da conexão e após clique em “Avançar”


Conectar a um Local de Trabalho
Digite o endereço da Internet com o qual se conectar
O administrador de rede pode lhe fornecer este endereço.
Endereço na Internet:
192.168.11.90
Nome do destino:
Conexão VPN
Usar um cartão inteligente
Permitir que outras pessoas usem esta conexão
Esta opção permite que qualquer pessoa com acesso a este computador use a conexão.
Não se conectar agora. Apenas configurar para permitir conexão posterior
Avançar
Cancelar

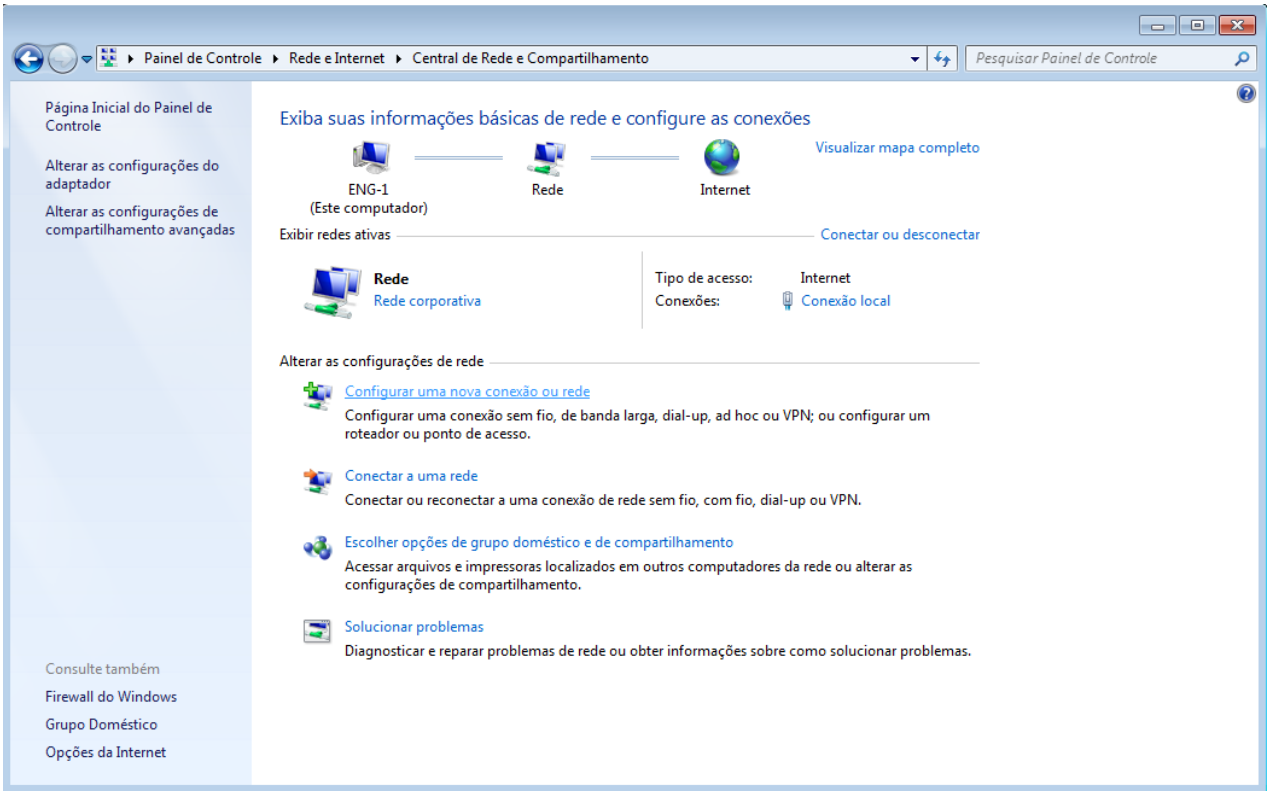
7 - Programe o usuário, a senha e o IP do destino e clique em “Conectar”.

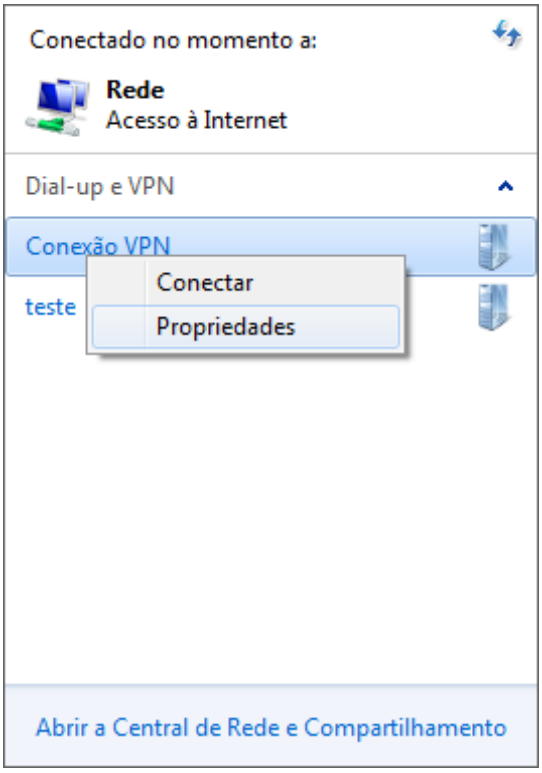


8 - Após aparecerá a conexão, mas essa conexão não irá funcionar pois será necessário configurar mais alguns itens. Clique em "Configurar a conexão assim mesmo"

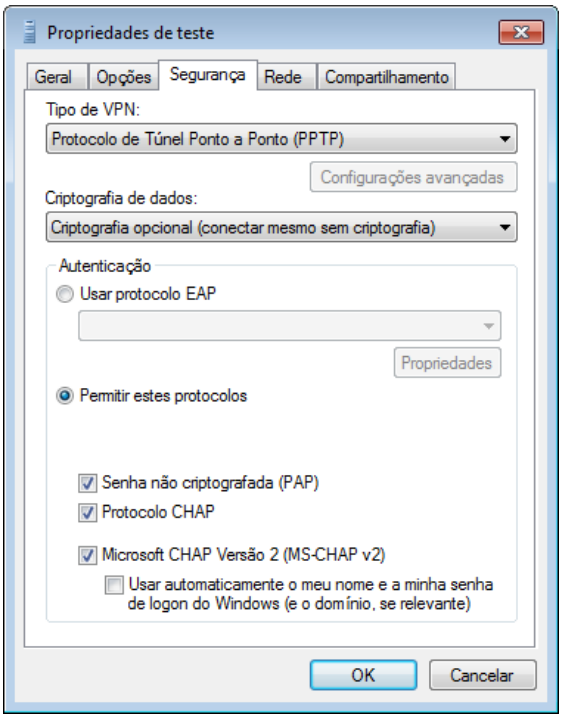

Conectar a um Local de Trabalho
A conexão falhou com erro 619
Não foi possível estabelecer uma conexão com o computador remoto; por isso, a porta usada para essa conexão foi fechada.
Tentar novamente
Configurar a conexão assim mesmo
Cancelar

9 - Entre no item "Conectar a uma rede" e com botão direito do mouse clique sobre a conexão configurada e selecione o item “propriedades”.

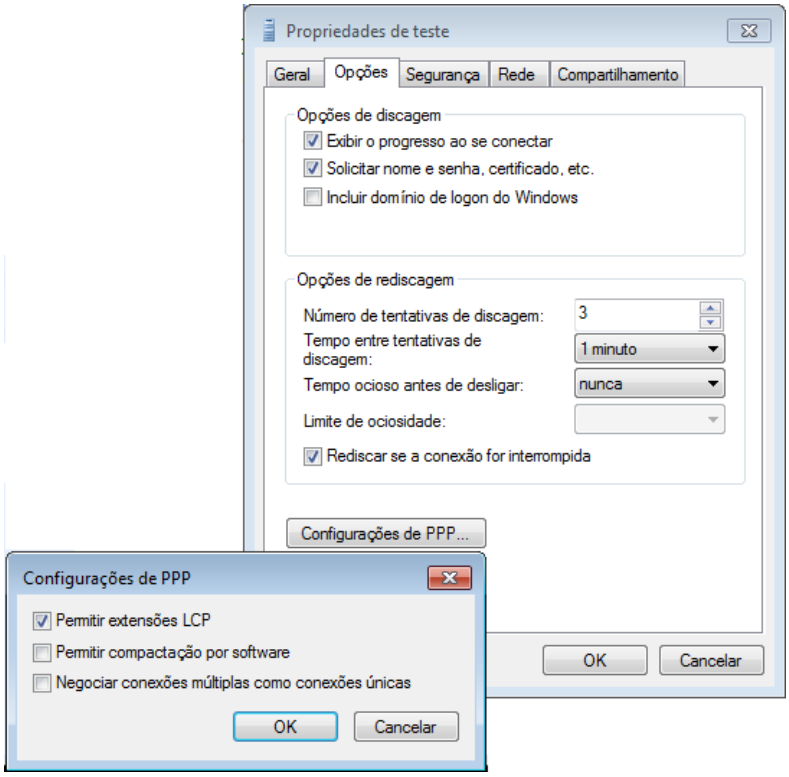

Painel de Controle ▸ Rede e Internet ▸ Central de Rede e Compartilhamento
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Alterar as configurações do adaptador
Alterar as configurações de compartilhamento avançadas
Exiba suas informações básicas de rede e configure as conexões
Visualizar mapa completo
ENG-1
(Este computador)
Rede
Internet
Exibir redes ativas
Conectar ou desconectar
Rede
Rede corporativa
Tipo de acesso: Internet
Conexões: Conexão local
Alterar as configurações de rede
Configurar uma nova conexão ou rede
Configurar uma conexão sem fio, de banda larga, dial-up, ad hoc ou VPN; ou configurar um roteador ou ponto de acesso.
Conectar a uma rede
Conectar ou reconectar a uma conexão de rede sem fio, com fio, dial-up ou VPN.
Escolher opções de grupo doméstico e de compartilhamento
Acessar arquivos e impressoras localizados em outros computadores da rede ou alterar as configurações de compartilhamento.
Solucionar problemas
Diagnosticar e reparar problemas de rede ou obter informações sobre como solucionar problemas.
Consulte também
Firewall do Windows
Grupo Doméstico
Opções da Internet



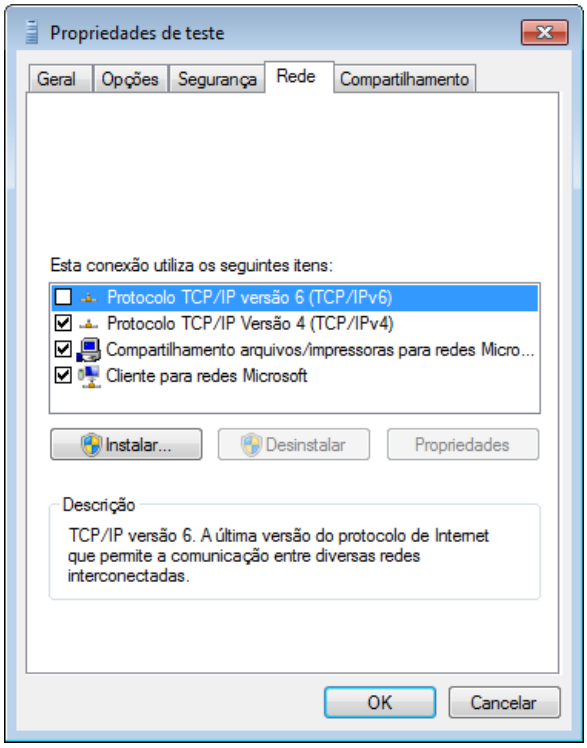
10 - Clique na aba "Segurança" e programe os itens conforme as telas abaixo. Após clique em “OK”



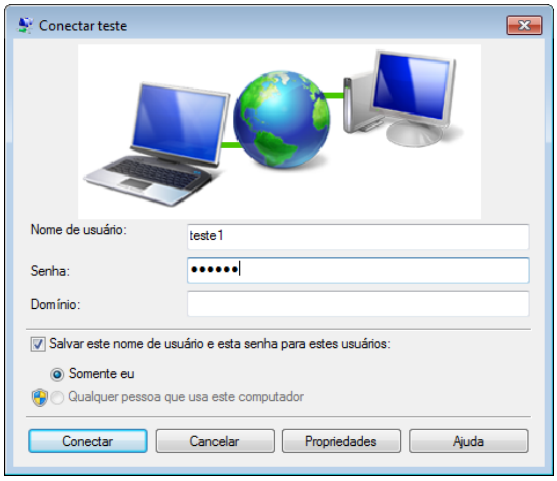
11 - Clique na aba "Opções" e programe os itens conforme as telas abaixo. Após clique em “OK”



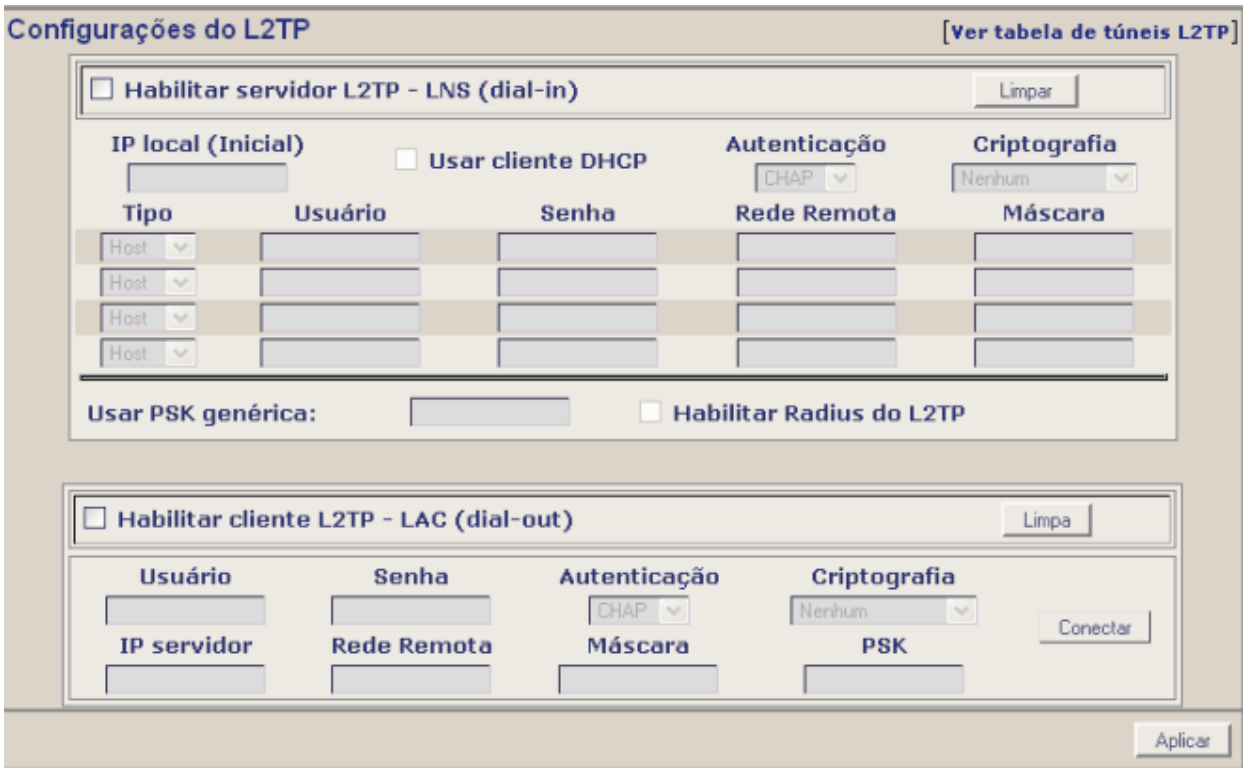
12 - Clique na aba "Rede" e programe os itens conforme as telas abaixo. Após clique em “OK”



13 - Configure usuário e senha. Após clique em “Conectar”.



3.4.2. Configurações do L2TP



A sigla L2TP significa protocolo de túnel de camada 2. É um protocolo que foi implementado pela IETF para resolver alguns problemas de segurança do PPTP e alguns problemas com o L2F. O protocolo utiliza os fundamentos do L2F, protocolo criado pelo fabricante Cisco. O L2TP tem como funcionalidade o transporte de protocolos de camada 2 do modelo OSI, como IP, IPX e NETBEUI, daí o seu nome. Também utiliza encapsulamento PPP, onde é possível utilizá-lo para fazer autenticação de usuários.

O L2TP utiliza a porta UDP 1701 para controle (RFC 2661). O L2TP não possui mecanismos de encriptação para tráfego de dados. Para resolver o problema de segurança utilizam o mesmo sobre outro protocolo seguro, o IPSEC.

No Gateway Digistar quando é utilizado o túnel IPSEC para fazer a encriptação dos dados utiliza-se o túnel IPSEC no modo túnel.

Como servidor permite :

- **Sem RADIUS e sem DHCP:** Permite até 4 conexões VPN. Configura-se um IP inicial fora do range do servidor DHCP e cada usuário que se conectar irá ganhar um IP entre o IP inicial e o IP inicial + 3. Assim se eu tiver 4 usuários User1, User2, User3 e User4, com o IP inicial 192.168.10.100, quando o usuário User1 se conectar irá ganhar o IP 192.168.10.100, quando o usuário User2 se conectar ganhará o IP 192.168.10.101, e assim até o User4 com o IP 192.168.10.103. Para que não haja conflito de IPs, é necessário usar o servidor DHCP (tela Rede e DHCP) com os limites de IPs que não colidam com os endereços do L2TP. Assim, no nosso exemplo, deveria ser configurado o servidor DHCP com IP final até 192.168.10.99 ou com o IP inicial a partir de 192.168.10.104.
- **Com RADIUS e sem DHCP:** Permite até 4 conexões. Semelhante a forma acima, com a diferença que os usuários e senhas devem ser colocados no servidor RADIUS, para o mesmo fazer a autenticação. Para configurar o servidor RADIUS seção **Erro! Fonte de referência não encontrada.**
- **Sem RADIUS e com DHCP:** Permite múltiplas conexões com até 4 usuários distintos. Não há mais configuração do IP inicial e os IP são fornecidos para os usuários através do servidor DHCP da rede. É a maneira mais fácil de estabelecer uma conexão L2TP. Desta forma, a cada conexão é fornecido um IP diferente, mesmo sendo o mesmo usuário. Assim, por exemplo, podemos criar um usuário "*vendedores*" e um usuário "*fornecedores*". Todos os vendedores podem acessar a rede privada usando o mesmo login "*vendedores*", assim como todos os fornecedores o login "*fornecedores*".
- **Com RADIUS e com DHCP.** Permite múltiplas conexões com até 4 usuários distintos. Irá usar o servidor DHCP para fornecer IPs e irá fazer autenticação usando o servidor RADIUS.

Existem duas formas de autenticação:

- PAP – (Protocolo de Autenticação por Senha) – É a forma de autenticação que envia o usuário e a senha em aberto na rede, sem nenhuma criptografia. É a maneira menos segura de autenticação.

- CHAP – (Protocolo de Autenticação de Desafio de Resposta) – Utiliza protocolo de codificação Message Digest 5 (MD5) de um só sentido. A senha é enviada de forma codificada.

  Quando é utilizada criptografia L2TP sobre IPSEC são utilizados como algoritmo de chave privada ou simétrica o 3DES, algoritmo de desafio SHA1 e como algoritmo de chave pública ou assimétrica o Diffie-Hellman Grupo 2 de 1024 bits (Ver mais detalhes na "Seção IPSEC"). Para fazer a autenticação das chaves :

  PSK (Pre- Shared Key, ou Chave pré-compartilhada): É o método em que as duas pontas possuem a mesma chave e que na hora de estabelecer o túnel as mesmas são verificadas. Normalmente são específicas para cada IP. Para facilitar o uso, no caso Cliente-LAN, foi criado um campo PSK genérica, que funciona para todos os usuários.

Para que se estabeleça um túnel IPSEC (no caso se usar o L2TP com criptografia) existe a necessidade de selecionar o tipo de identificador a ser usado pelo servidor. Se a empresa possuir um IP fixo (p. exemplo 200.200.200.200) e estiver selecionado o campo "Usar IP da WAN" para que a discagem funcione, a conexão deve discar exclusivamente para este número IP. Se estiver sendo usado o DNS dinâmico no Gateway Digistar podemos usar o campo "Usar FQDN do DDNS" e assim a conexão pode ser estabelecida discando para um nome ou FQDN (p. exemplo ip.do.servidor.com). Se estiver atrás de outra rede privada, ou outra máquina que faz o DNS dinâmico é possível usar a opção "Usar FQDN ou IP específico" e colocar outro identificador.

Com o L2TP é possível criar conexões do tipo Cliente-LAN ou LAN-to-LAN. A forma de uso é definida pelo campo TIPO. Se o campo estiver como *rede* irá se estabelecer uma conexão do tipo LAN-to-LAN, assim como se estiver como *host* irá se estabelecer uma conexão do tipo Cliente-LAN. Para conexão do tipo LAN-to-LAN é necessário informar o número de rede remota e a máscara da rede remota. Vale lembrar que é necessário que as redes privadas das máquinas sejam diferentes para que o túnel LAN-to-LAN se estabeleça.

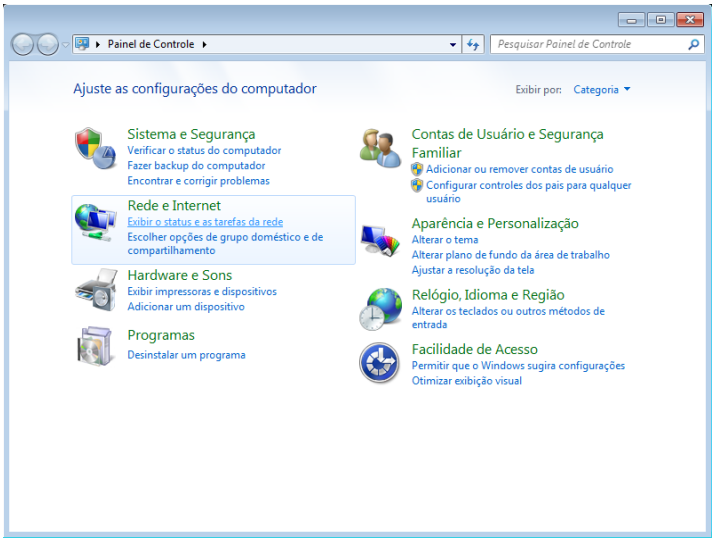
O Gateway Digistar pode funcionar como cliente L2TP, também chamado de LAC. Assim o Gateway Digistar irá fazer a discagem para outra máquina. Basta entrar com as configurações, aplicá-las e clicar no botão CONECTAR. No Gateway Digistar também pode ser habilitado como um servidor L2TP.

> **Importante:** *No Gateway Digistar somente é possível estabelecer um túnel L2TP seguro como cliente com o uso de PSK usando IPSEC como criptografia.*

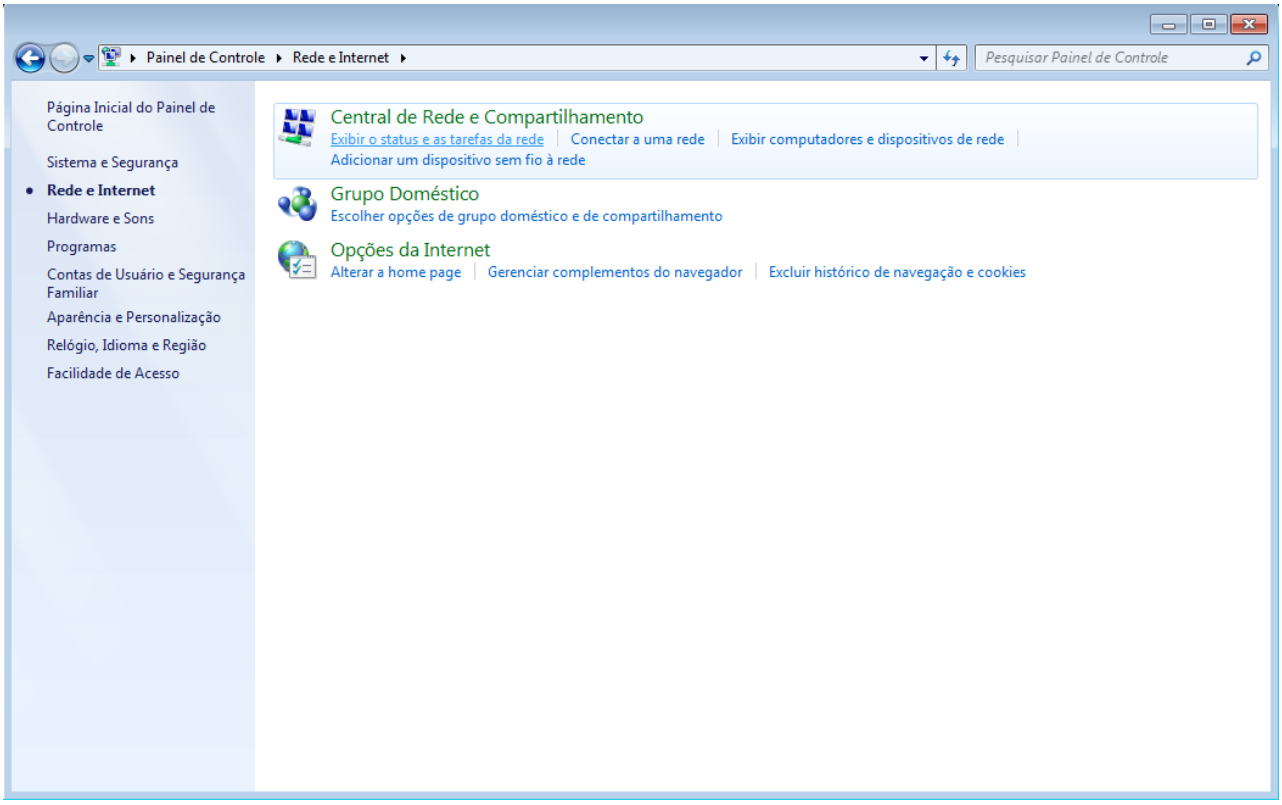
Para ver quais os túneis que estão ativos no momento, basta ir na opção "Ver tabela de túneis L2TP".

Os passos para fazer o túnel em ambiente Windows7 são:

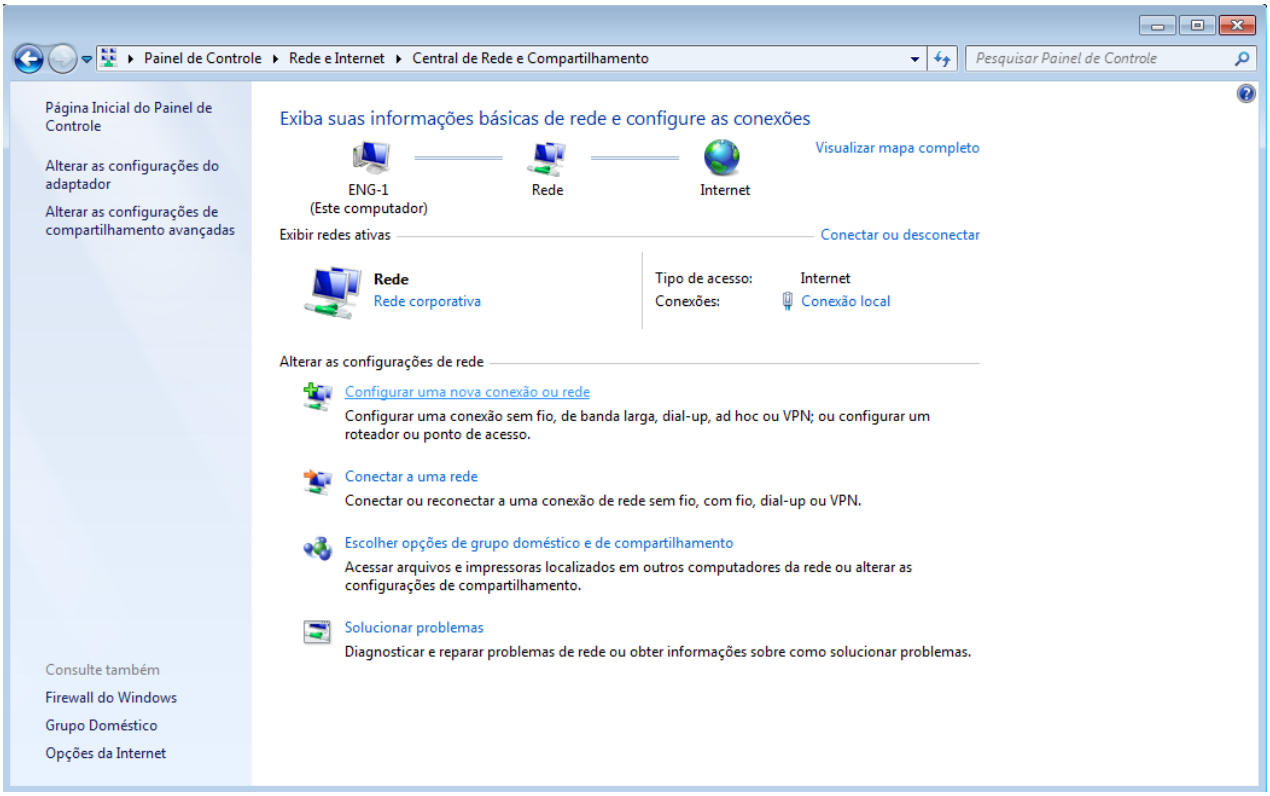
1 - Vá em "Painel de controle" e clique em "Rede e Internet"


Painel de Controle
Pesquisar Painel de Controle
Ajuste as configurações do computador
Exibir por: Categoria
Sistema e Segurança
Verificar o status do computador
Fazer backup do computador
Encontrar e corrigir problemas
Rede e Internet
Exibir o status e as tarefas da rede
Escolher opções de grupo doméstico e de compartilhamento
Hardware e Sons
Exibir impressoras e dispositivos
Adicionar um dispositivo
Programas
Desinstalar um programa
Contas de Usuário e Segurança Familiar
Adicionar ou remover contas de usuário
Configurar controles dos pais para qualquer usuário
Aparência e Personalização
Alterar o tema
Alterar plano de fundo da área de trabalho
Ajustar a resolução da tela
Relógio, Idioma e Região
Alterar os teclados ou outros métodos de entrada
Facilidade de Acesso
Permitir que o Windows sugira configurações
Otimizar exibição visual

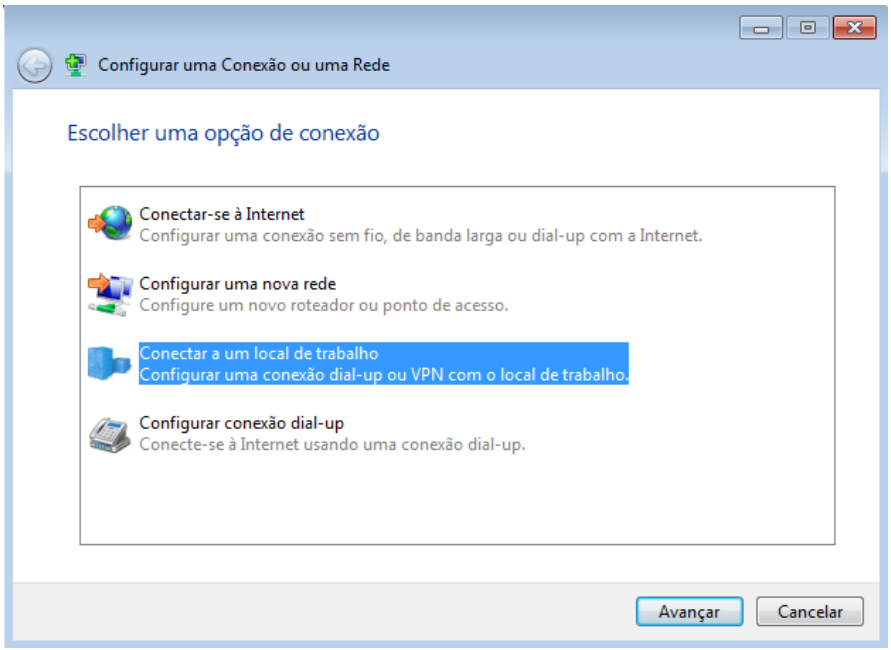
2 - Clique em "Exibir o status e as tarefas da Rede"


Painel de Controle
Rede e Internet
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Sistema e Segurança
Rede e Internet
Hardware e Sons
Programas
Contas de Usuário e Segurança Familiar
Aparência e Personalização
Relógio, Idioma e Região
Facilidade de Acesso
Central de Rede e Compartilhamento
Exibir o status e as tarefas da rede
Conectar a uma rede
Exibir computadores e dispositivos de rede
Adicionar um dispositivo sem fio à rede
Grupo Doméstico
Escolher opções de grupo doméstico e de compartilhamento
Opções da Internet
Alterar a home page
Gerenciar complementos do navegador
Excluir histórico de navegação e cookies

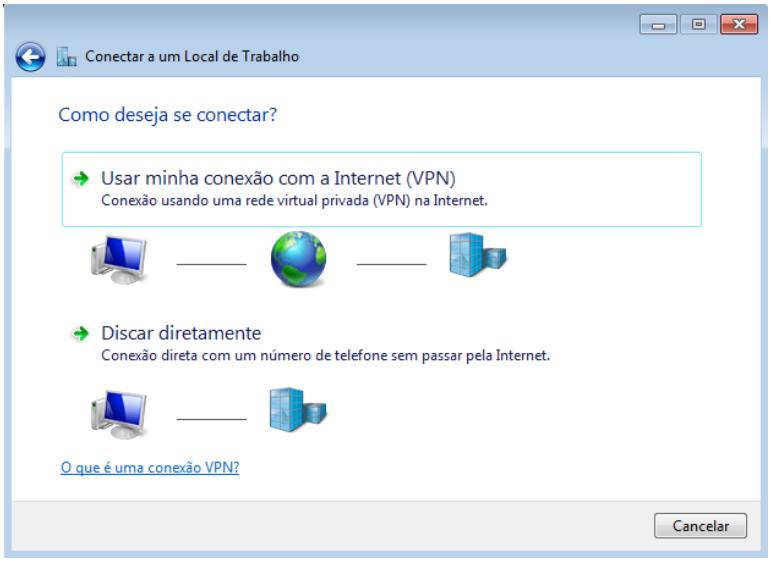
3 - Clique em "Configurar uma nova conexão ou rede"


Painel de Controle ▸ Rede e Internet ▸ Central de Rede e Compartilhamento
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Alterar as configurações do adaptador
Alterar as configurações de compartilhamento avançadas
Exiba suas informações básicas de rede e configure as conexões
Visualizar mapa completo
ENG-1
(Este computador)
Rede
Internet
Exibir redes ativas
Conectar ou desconectar
Rede
Rede corporativa
Tipo de acesso: Internet
Conexões: Conexão local
Alterar as configurações de rede
Configurar uma nova conexão ou rede
Configurar uma conexão sem fio, de banda larga, dial-up, ad hoc ou VPN; ou configurar um roteador ou ponto de acesso.
Conectar a uma rede
Conectar ou reconectar a uma conexão de rede sem fio, com fio, dial-up ou VPN.
Escolher opções de grupo doméstico e de compartilhamento
Acessar arquivos e impressoras localizados em outros computadores da rede ou alterar as configurações de compartilhamento.
Solucionar problemas
Diagnosticar e reparar problemas de rede ou obter informações sobre como solucionar problemas.
Consulte também
Firewall do Windows
Grupo Doméstico
Opções da Internet

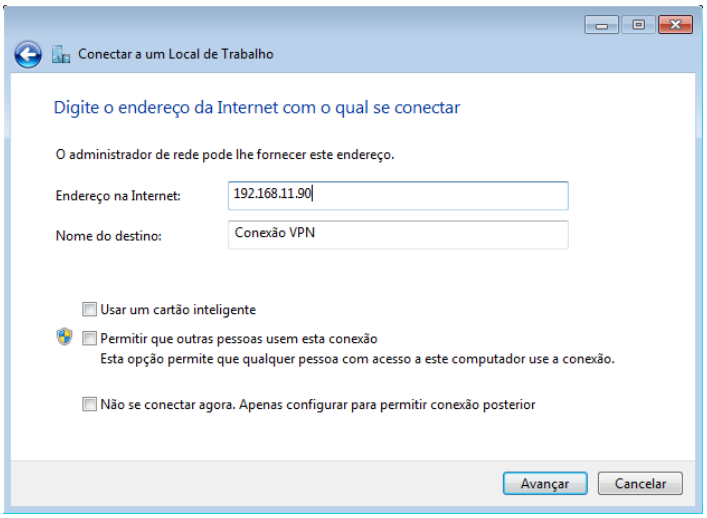
4 - Clique em "Conectar a um local de trabalho" e depois em "avançar"


Configurar uma Conexão ou uma Rede
Escolher uma opção de conexão
Conectar-se à Internet
Configurar uma conexão sem fio, de banda larga ou dial-up com a Internet.
Configurar uma nova rede
Configure um novo roteador ou ponto de acesso.
Conectar a um local de trabalho
Configurar uma conexão dial-up ou VPN com o local de trabalho.
Configurar conexão dial-up
Conecte-se à Internet usando uma conexão dial-up.
Avançar
Cancelar

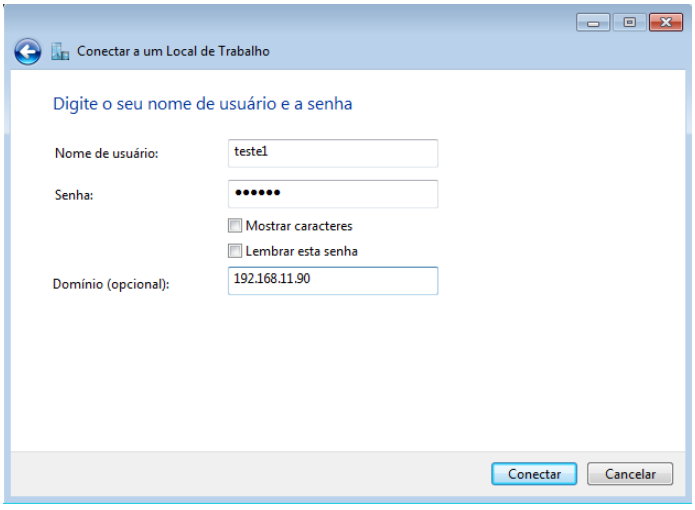
5 - Clique em "Usar minha conexão com a internet (VPN)"


Conectar a um Local de Trabalho
Como deseja se conectar?
Usar minha conexão com a Internet (VPN)
Conexão usando uma rede virtual privada (VPN) na Internet.
Discar diretamente
Conexão direta com um número de telefone sem passar pela Internet.
O que é uma conexão VPN?
Cancelar

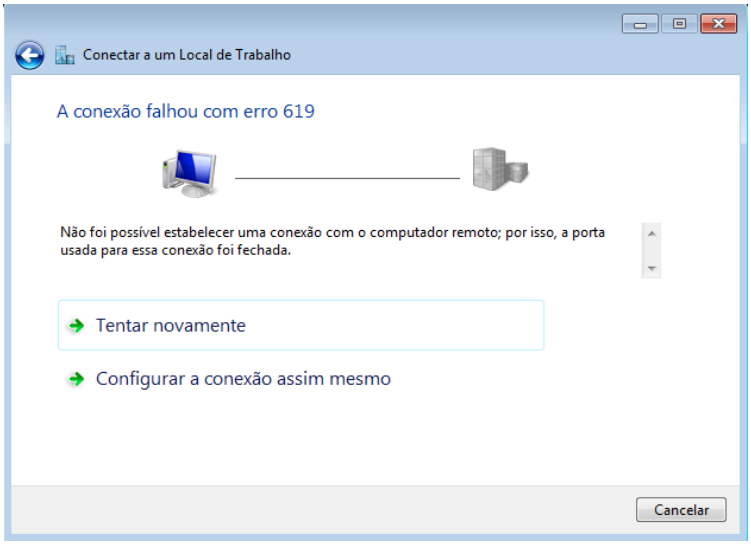
6 - Configure o IP onde será conectada a VPN e o nome da conexão e após clique em “Avançar”


Conectar a um Local de Trabalho
Digite o endereço da Internet com o qual se conectar
O administrador de rede pode lhe fornecer este endereço.
Endereço na Internet:
192.168.11.90
Nome do destino:
Conexão VPN
Usar um cartão inteligente
Permitir que outras pessoas usem esta conexão
Esta opção permite que qualquer pessoa com acesso a este computador use a conexão.
Não se conectar agora. Apenas configurar para permitir conexão posterior
Avançar
Cancelar

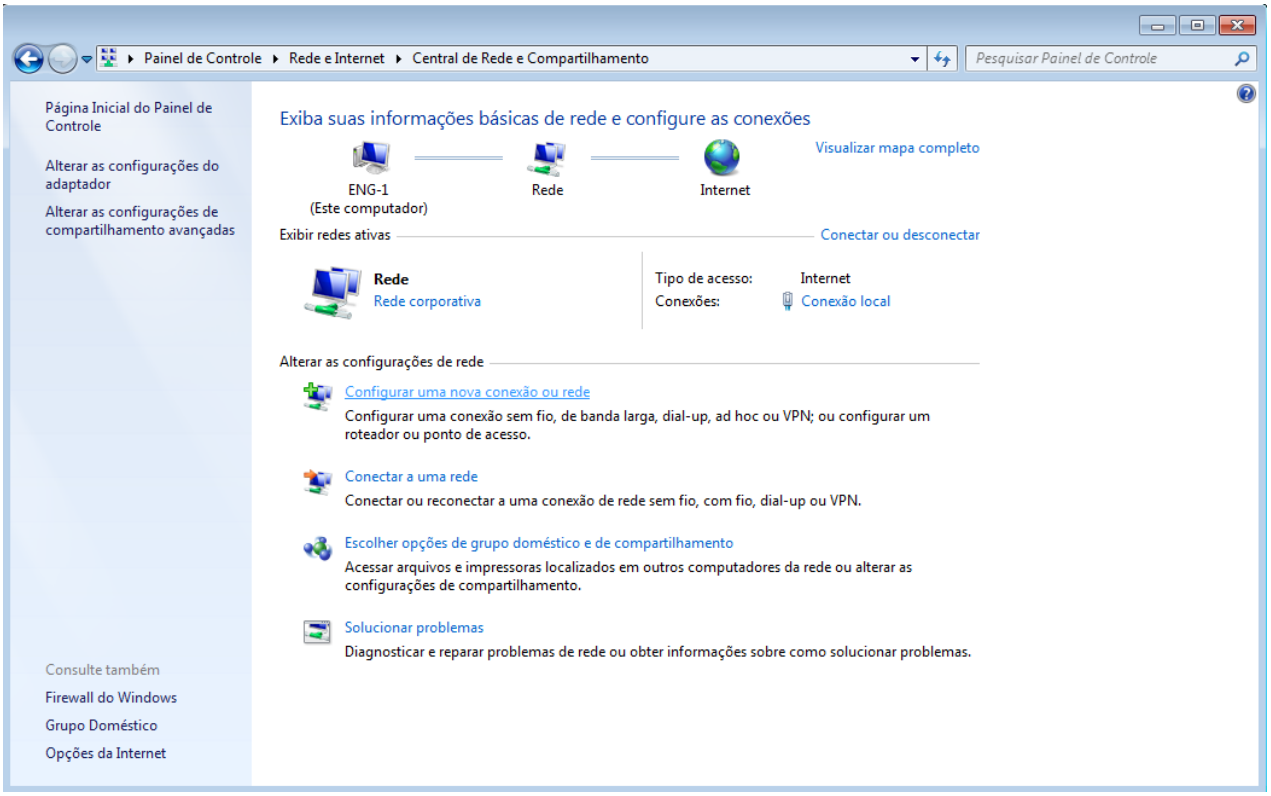
7 - Programe o usuário, a senha e o IP do destino e clique em “Conectar”.

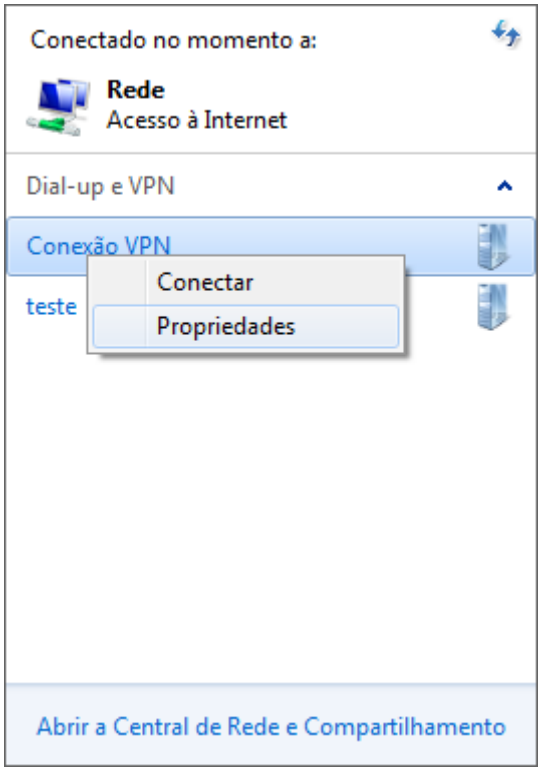


8 - Após aparecerá a conexão, mas essa conexão não irá funcionar pois será necessário configurar mais alguns itens. Clique em "Configurar a conexão assim mesmo"

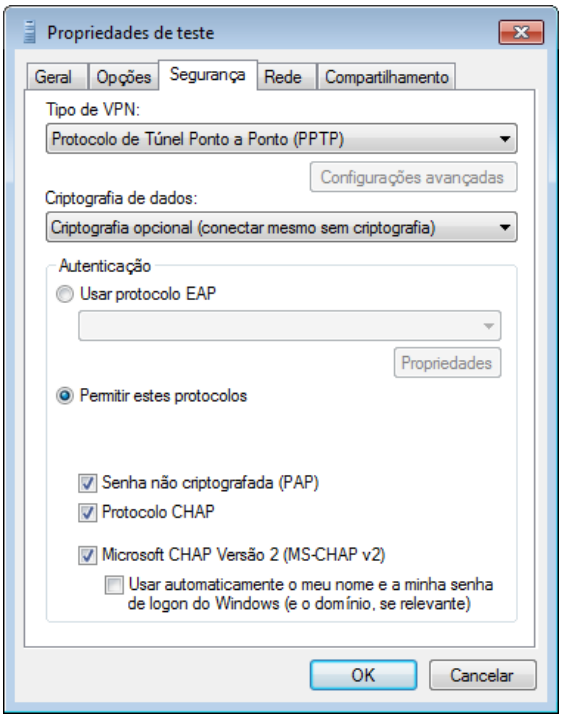

Conectar a um Local de Trabalho
A conexão falhou com erro 619
Não foi possível estabelecer uma conexão com o computador remoto; por isso, a porta usada para essa conexão foi fechada.
Tentar novamente
Configurar a conexão assim mesmo
Cancelar

9 - Entre no item "Conectar a uma rede" e com botão direito do mouse clique sobre a conexão configurada e selecione o item “propriedades”.

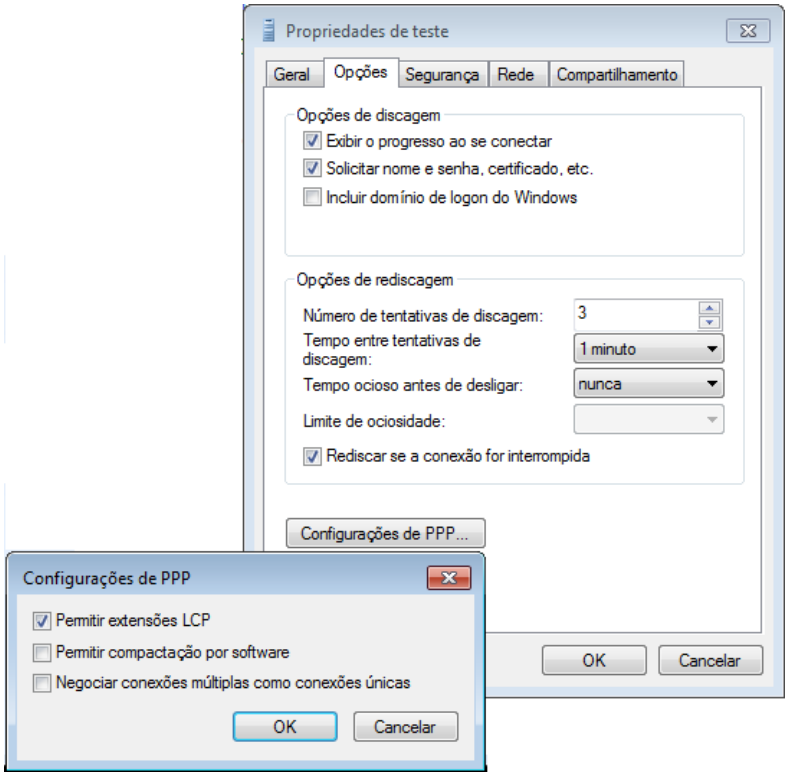

Painel de Controle ▸ Rede e Internet ▸ Central de Rede e Compartilhamento
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Alterar as configurações do adaptador
Alterar as configurações de compartilhamento avançadas
Exiba suas informações básicas de rede e configure as conexões
Visualizar mapa completo
ENG-1
(Este computador)
Rede
Internet
Exibir redes ativas
Conectar ou desconectar
Rede
Rede corporativa
Tipo de acesso: Internet
Conexões: Conexão local
Alterar as configurações de rede
Configurar uma nova conexão ou rede
Configurar uma conexão sem fio, de banda larga, dial-up, ad hoc ou VPN; ou configurar um roteador ou ponto de acesso.
Conectar a uma rede
Conectar ou reconectar a uma conexão de rede sem fio, com fio, dial-up ou VPN.
Escolher opções de grupo doméstico e de compartilhamento
Acessar arquivos e impressoras localizados em outros computadores da rede ou alterar as configurações de compartilhamento.
Solucionar problemas
Diagnosticar e reparar problemas de rede ou obter informações sobre como solucionar problemas.
Consulte também
Firewall do Windows
Grupo Doméstico
Opções da Internet



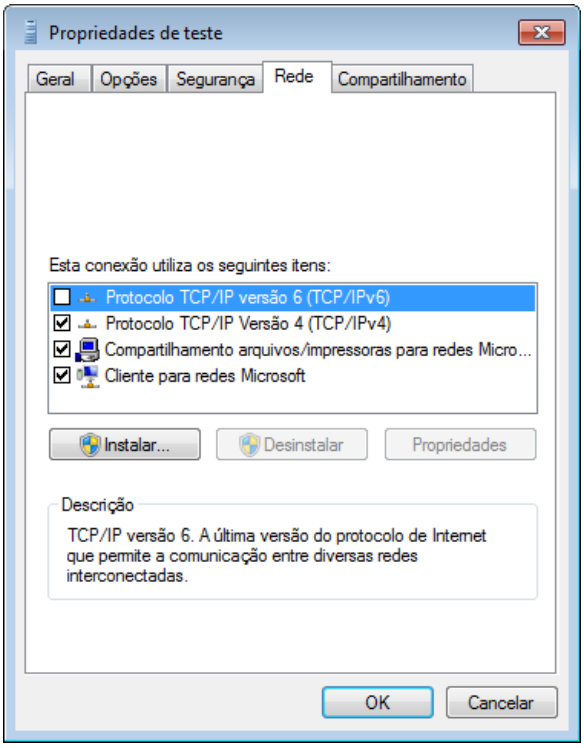
10 - Clique na aba "Segurança" e programe os itens conforme as telas abaixo. Após clique em “OK”



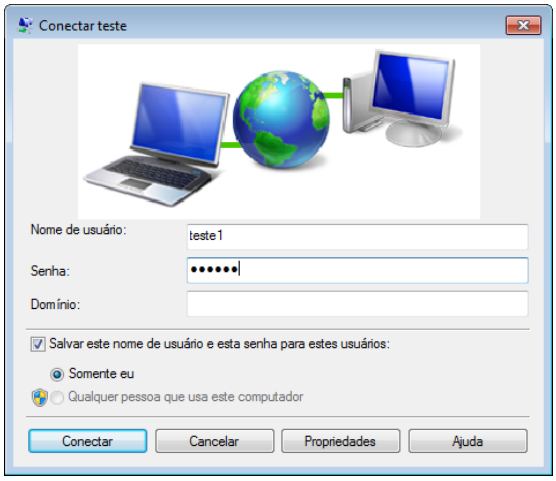
11 - Clique na aba "Opções" e programe os itens conforme as telas abaixo. Após clique em “OK”



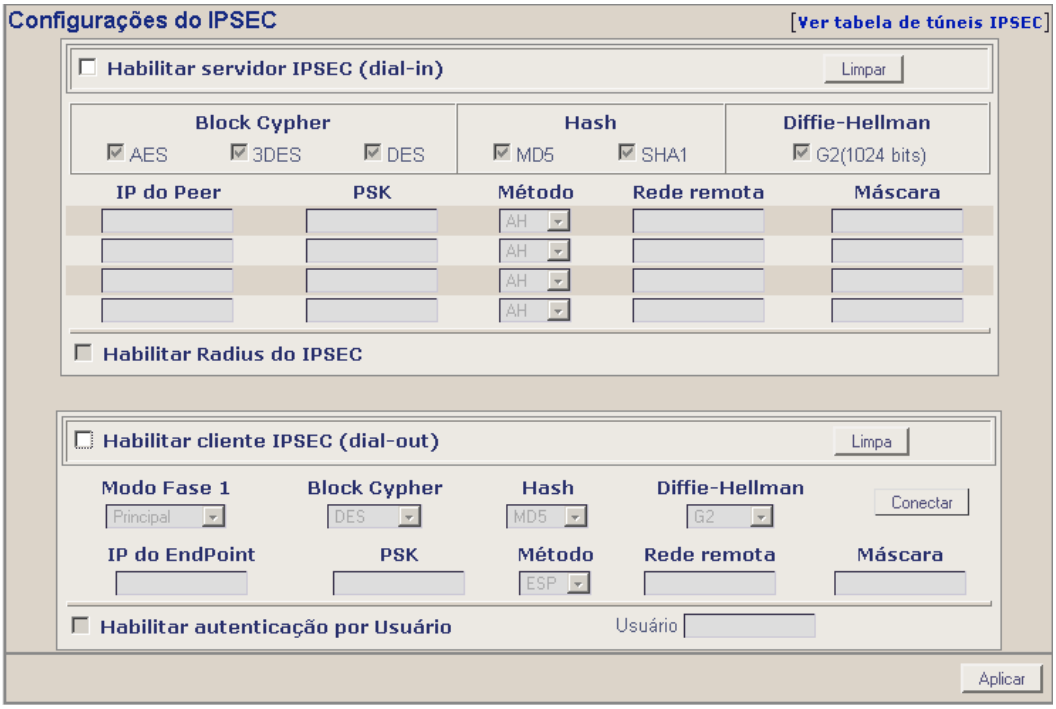
12 - Clique na aba "Rede" e programe os itens conforme as telas abaixo. Após clique em “OK”



13 - Configure usuário e senha. Após clique em “Conectar”.



3.4.3. Configurações do IPSEC



O IPSec ou IP seguro é um conjunto de protocolos desenvolvido pelo grupo de segurança do IETF para garantir autenticidade, confidenciabilidade e integridade dos dados. Os protocolos IPSec são de camada 3, ou seja, fazem IP sobre IP. Outra função do IPSec é o gerenciamento e troca de chaves IKE (Internet Key Exchange- RFC 2409).

O IPSec possui dois modos de operação:

Modo transporte: Somente os dados são criptografados. Assim a composição final do pacote IP será: Cabeçalho original + Cabeçalho IPSec + Dados criptografados.

Modo túnel: Tanto o cabeçalho quanto os dados são criptografados. Assim a composição do pacote IP será: Novo cabeçalho IP + Cabeçalho IPSec + Cabeçalho e dados criptografados.

O Gateway Digistar também permite utilizar o modo de túnel.

Como falado anteriormente o IPSec é um conjunto de protocolos, composto de:

AH (Autenticação de Cabeçalho – RFC 2402): Fornece autenticação e integridade dos dados, porém não fornece confidencialidade;
ESP (Dados encapsulados – RFC 2406): Fornece autenticação e confidencialidade dos dados através de criptografia, porém não oferece integridade.

IKE (Troca de chaves pela Internet – RFC 2409): Utilizado para troca de Associações Seguras (SA), ou seja, verifica quais os tipos de criptografia disponíveis em ambos os lados, e também gerencia os tipos de chaves disponíveis.

Existem três métodos de autenticação:

- PSK (Pre-Shared Key, ou Chave pré-compartilhada): É o método em que as duas pontas possuem a mesma chave e na hora de estabelecer o túnel as mesmas são verificadas.
- Certificados: É o método em que um certificado da maquina A é instalado na máquina B e vice-versa. Também é conhecido como uma autenticação assimétrica, pois as chaves para criptografar e para descriptografar são diferentes, garantindo maior segurança. Pela dificuldade de instalação de certificados o Gateway Digistar **não** trabalha com certificados usando IPSec.
- X-Auth ou Híbrida: Autenticação será feita usando uma chave pré-compartilhada para um usuário específico e não para um IP como na PSK.

O túnel IPSec é estabelecido sob demanda e não de forma compulsória, ou seja, quando for feito um Peer, por exemplo, *"ip.remoto"* que possui uma rede LAN 192.168.1.0, com máscara 255.255.255.0, acessando qualquer IP 192.168.1.X, o IPSec tentará criar o túnel. Se o túnel ficar em desuso o túnel deixará de existir. Vale lembrar que é necessário que as redes privadas das máquinas sejam diferentes para que o túnel LAN-to-LAN se estabeleça.

Para que se estabeleça um túnel IPSEC (caso se use o L2TP com criptografia) existe a necessidade de selecionar o tipo de identificador do servidor. Se a empresa possuir um IP fixo (p. exemplo 200.200.200.200) e estiver selecionado o campo "Usar IP da WAN" para que a discagem funcione, a conexão deve discar exclusivamente para este número IP. Se estiver sendo usado o DNS dinâmico no Gateway Digistar podemos usar o campo "Usar FQDN do DDNS" e assim a conexão pode ser estabelecida discando para um nome ou FQDN (p. exemplo ip.do.servidor.com). Se estiver atrás de outra rede privada, ou outra máquina faz o DNS dinâmico é possível usar a opção "Usar FQDN ou IP específico" e colocar outro identificador.

Como o túnel é criado sob demanda, qualquer Peer colocado no campo "Dial–in", pode ser usado para começar o túnel. Qualquer serviço que tentar acessar o IP da LAN do Peer remoto (por exemplo, ping 192.168.10.1), estabelecerá a conexão.

Se houver a necessidade de forçar a conexão, ou de usar o IPSec no modo Híbrido, existe o campo "Dial-out" , onde é possível usar o botão "Conectar" ou a autenticação por usuário..

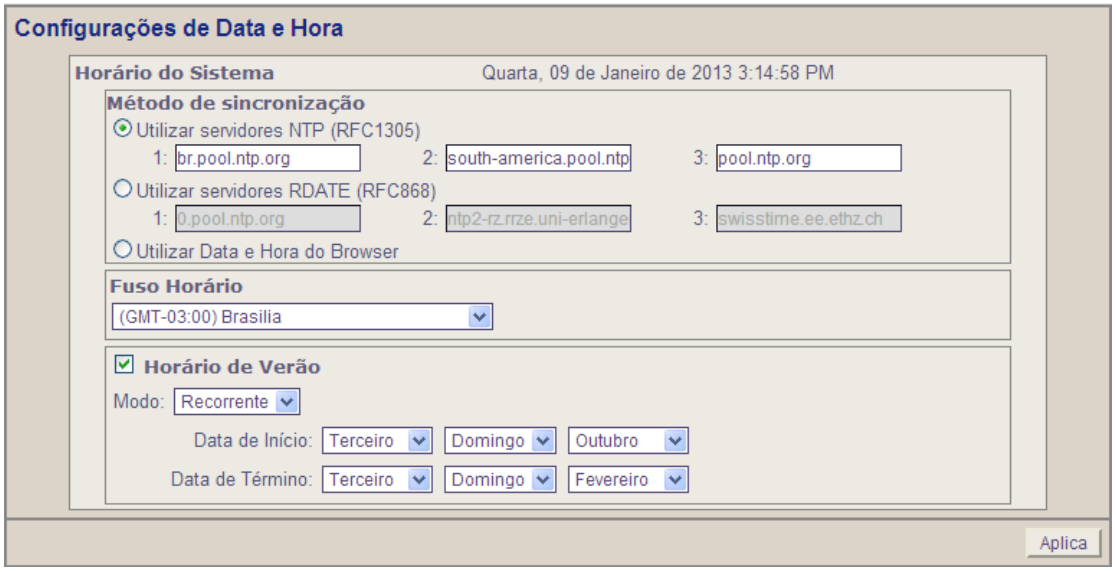
Para ver quais os túneis que estão ativos no momento, basta ir na opção "Ver tabela de túneis IPSEC".

Os algoritmos de cryptografia (block cypher) utilizados são o DES, 3DES e AES. Os algoritmos de embaralhamento (hash) são o MD5 e o SHA1. O algoritmo de exponenciação é o Diffie-Hellman grupo 2 (1024 bits) (chave simétrica).

Para o cliente de um túnel IPSEC há a opção de definir qual o algoritmo de criptografia (block cypher) e o algoritmo de embaralhamento (hash) desejável para a conexão. Também é possível definir o modo como será feita a troca de chaves pela Internet (IKE). A conexão é estabelecida em duas fases, sendo que na primeira (Modo Fase 1) é possível mandar todas as informações (6 pacotes) ou metade delas (3 pacotes). Quando se envia todas as informações é chamado de modo principal, quando se envia metade chamamos modo agressivo. Para garantir maior segurança o modo principal é recomendado.

3.5. Serviços

3.5.1. Configurações de Data e Hora



Método de Sincronização

O relógio do Gateway Digistar pode ser sincronizado a partir de três tipos de fonte de data e hora: servidores **NTP** (RFC1305), servidores de **RDATE** (RFC868), e também o próprio **browser.**

Para que possa sincronizar data e hora através de servidores de NTP ou RDATE, o Gateway Digistar deve estar com a rede da WAN configurada e com acesso a pelo menos um dos servidores que devem ser especificados. A sincronização é realizada assim que as configurações são aplicadas e também a cada reinicialização do Gateway Digistar. Se os servidores estiverem indisponíveis por qualquer motivo então será realizada uma nova tentativa de atualização de cinco em cinco minutos até que o relógio seja sincronizado com sucesso.

Para o caso de não haver disponibilidade de alguma máquina com servidores NTP ou RDATE segue abaixo uma lista de servidores públicos na internet. Deve-se notar que estes servidores são oferecidos voluntariamente e não têm garantias de precisão de relógio nem de disponibilidade de acesso. Uma lista maior e atualizada de servidores NTP pode ser encontrada em http://ntp.isc.org.

NTP	RDATE
br.pool.ntp.org	time.nist.gov
south-america.pool.ntp.org	time-a.nist.gov
pool.ntp.org	time-b.nist.gov
0.pool.ntp.org	time-a.timefreq.bldrdoc.gov, time-b.timefreq.bldrdoc.gov, time-c.timefreq.bldrdoc.gov
1.pool.ntp.org	utcnist.colorado.edu
2.pool.ntp.org	nist1.symmetricom.com

Para atualizar a data e a hora pelo navegador basta ajustar o relógio da máquina cliente do Configurador Web Digistar e aplicar a configuração. Utilizando o ajuste de data e hora através do browser será necessário fazer a sincronização através do configurador cada vez que o Gateway Digistar for inicializado.

Fuso horário

Selecione o fuso horário correspondente à sua região. Os fusos horários dos estados brasileiros são apresentados abaixo:

Acre, Amazonas (oeste)	GMT-5:00
Amazonas (leste), Mato Grosso, Mato Grosso do Sul, Pará (oeste), Rondônia, Roraima	GMT-4:00
Alagoas, Amapá, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Pará (oeste), Paraíba, Paraná, Pernambuco (oeste), Piauí, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, São Paulo, Sergipe, Tocantins	GMT-3:00
Pernambuco (leste)	GMT-2:00

Horário de verão

As datas de início e fim do horário de verão estão sujeitas à legislação vigente na região. Para configurar duração do horário de verão corrente no Brasil consulte os decretos do governo disponíveis no site http://pcdsh01.on.br/DecHV.html

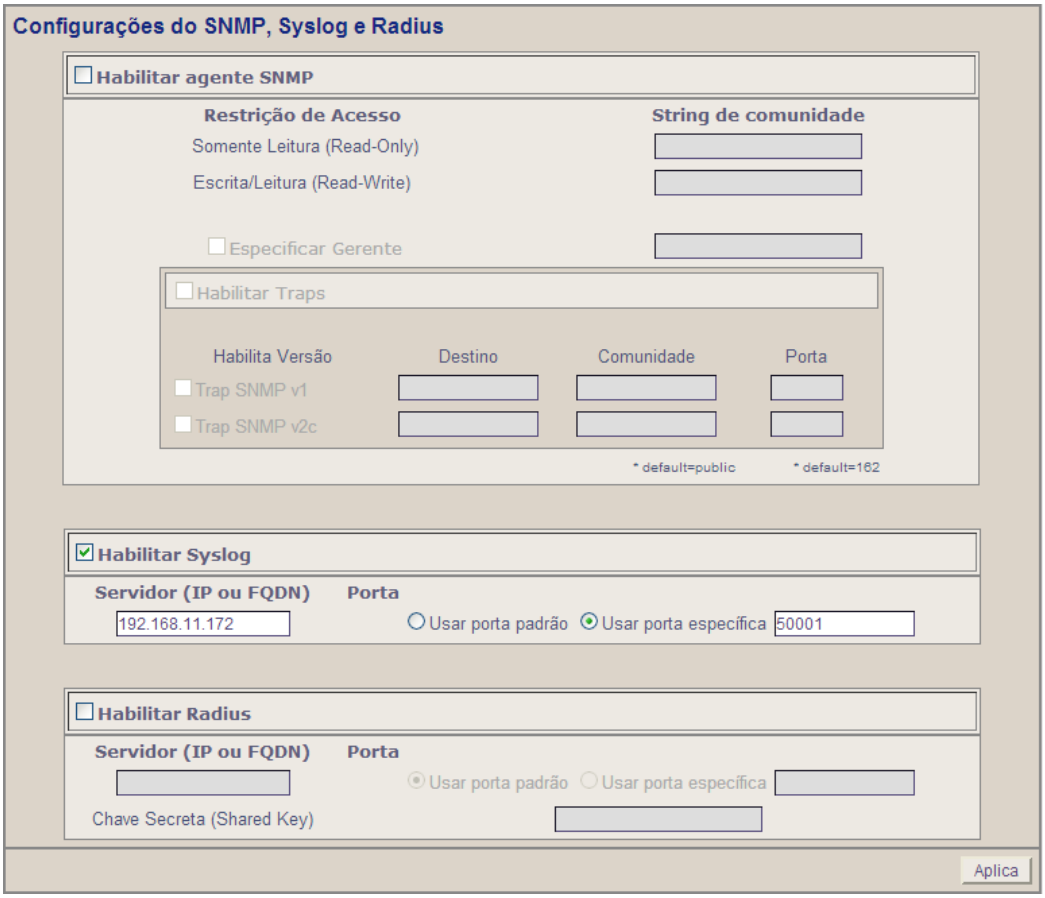
Observação: "Quando mudar o fuso horário ou as datas do horário de verão, o equipamento deverá ser reiniciado".

3.5.2. Configurações de SNMP/Syslog e Radius

Habilitar RADIUS

O RADIUS (Remote Authentication Dial In User Service) é um protocolo especificado pela RFC – 2865 para fazer autenticação, autorização e verificação de contas de usuários. O servidor Radius, se habilitado, será o mesmo utilizado para todos os tipos de VPN.

O servidor RADIUS deve estar em uma máquina da rede interna. A porta padrão de uso é a 1812, mas há a opção de mudar a porta de saída.



Habilitar agente SNMP

O Gateway Digistar possui ferramentas convencionais de gerenciamento como o agente SNMP (Simple Network Management Protocol). O SNMP é um protocolo, na camada de aplicação, para o gerenciamento de redes TCP/IP. O agente SNMP do Gateway Digistar tem suporte às versões v1 e v2c do SNMP, implementando as MIBs:

MIBs padrões:

- MIB-II (RFC 1213 e revisões subsequentes): permite o monitoramento de diversas informações da rede, tais como estado das interfaces de rede e estatísticas de uso dos protocolos TCP/UDP, entre outras.
- RTP-MIB (RFC 2959): possibilita monitorar o desempenho das ligações VoIP (ex.: jitter, pacotes enviados/recebidos e perdidos, etc).
- DS1-MIB (RFC 4805): permite monitorar a interface E1 (estatísticas de erros e de performance do link, tais como escorregamento, perda de sincronismo de quadro, entre outras, e notificações de mudanças do estado do link (com/sem erro)
- Host Resources (RFC 1514 and 2790): permite monitorar o sistema, como por exemplo, a carga de processamento da CPU.
- RMON (alarm, event, ethernet history e statistcs): permite obter histórico e estatísticas da rede e gerar notificações (traps) a partir de limiares (thresholds) pré-definidos.

Restrições de Acesso: Por motivos de segurança é possível especificar comunidades (String de comunidade) de somente leitura ou comunidades que permitam também escritas. Caso sejam definidas comunidades equivalentes nos dois modos, prevalecerá a opção de somente leitura e a escrita não será permitida.

Especificar Gerente: Para garantir que somente uma máquina possa gerenciar é possível colocar o IP ou FQDN (nome do domínio, www.digistar.com.br, por exemplo) de um gerente específico.

Habilitar Traps: Além de consultas ao Gateway Digistar o agente SNMP também permite o envio de alarmes (Traps/Notificações) sobre determinados eventos ocorridos no equipamento. São enviadas Traps, conforme a MIB II, quando o agente é iniciado e finalizado, e quando é recebida uma requisição SNMP v1 usando uma comunidade com um nome desconhecido. Também são enviadas Traps quando é modificado o estado do tronco E1, como definido em DS1-MIB (RFC 4805). É possível habilitar o envio de Traps nas versões SNMP v1 e SNMP v2. Caso for ativada as duas opções o agente do Gateway Digistar enviará Traps em ambas as versões. Em cada versão habilitada deve-se definir o IP ou FQDN e a Porta de destino das Traps. Se não for definido um valor para a porta será utilizada a porta padrão 162. Quando necessário também é possível definir uma Comunidade específica às Traps (por padrão envia-se com a comunicada "public").

Habilitar SYSLOG

O syslog (RFC – 3164) é um protocolo de transmissão de eventos e notificações (Logs) pela internet. Foi desenvolvido inicialmente na University of Califórnia Berkeley Software Distribution (BSD). O Syslog utiliza protocolo UDP e a porta 514 como padrão de saída. Também há a opção de trocar a porta de saída.

Habilitar RADIUS

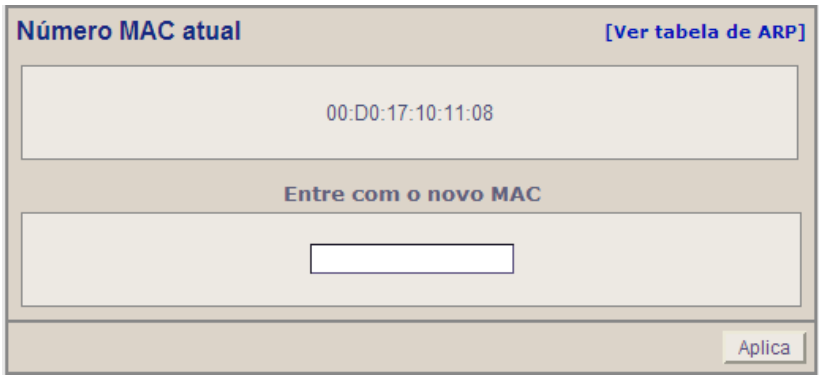
O RADIUS (Remote Authentication Dial In User Service) é um protocolo especificado pela RFC – 2865 para fazer autenticação, autorização e verificação de contas de usuários. O servidor Radius, se habilitado, será o mesmo utilizado para todos os tipos de VPN.

O servidor RADIUS deve estar em uma máquina da rede interna. A porta padrão de uso é a 1812, mas há a opção de mudar a porta de saída.

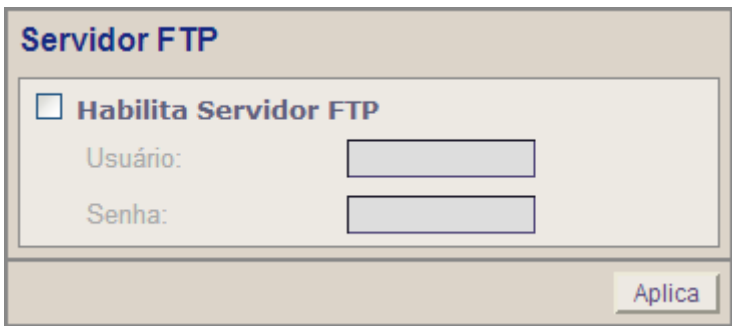
3.5.3. Troca do MAC

O Gateway Digistar vem programado de fábrica com um número MAC. Caso haja colisão do número com outro da rede, existe a possibilidade de trocar por outro MAC. Para que a operação de troca de número MAC seja feita com sucesso, após a troca, o Gateway Digistar deve ser reinicializado.

Também existe a opção de verificar a tabela ARP (Resolução de endereços com os MAC) visível nas interfaces de rede, clicando na opção *"Ver tabela de ARP"*.



3.5.4. Servidor FTP



Para acessar o arquivo com os bilhetes de tarifação (bilhetes_ftp.txt) via “File Transfer Protocol” (FTP), é necessário habilitar e configurar um usuário com sua respectiva senha no configurador WEB Digistar. Após feita a conexão, com o registro do usuário, é permitido ler e apagar o arquivo.

O arquivo é salvo em uma memória flash, i.e., não é perdido se eventualmente o equipamento for desligado, seja propositadamente ou por falta de energia elétrica.

Porta default FTP: 21

Campos:

ORIGEM						DESTINO								
NÚMERO FROM	ESPAÇO	NÚMERO TO	ESPAÇO	ROTA ORIGEM	ESPAÇO	NÚMERO FROM	ESPAÇO	NÚMERO TO	ESPAÇO	ROTA DESTINO	ESPAÇO	DATA/HORA	ESPAÇO	DURAÇÃO
até 20 dígitos	01	até 20 dígitos	01	04 dígitos	01	até 20 dígitos	01	até 20 dígitos	01	04 dígitos	01	16 dígitos	01	08 dígitos

Origem:

NÚMERO FROM: Até 20 caracteres.
Contém a identificação do usuário de um dos pontos remotos ou o IDC da ligação de entrada.

***ESPAÇO*:** 1 caractere com espaço em branco para separar o número From do número To.

NÚMERO TO: Até 20 caracteres.
Contém o número discado que o gateway recebeu na interface de entrada.

ESPAÇO: 1 caractere com espaço em branco para separar a rota de origem do número To.

ROTA ORIGEM: 4 caracteres
Identifica a rota de origem: <Interface> + <Grupo Entrada, Sip Integrado ou Conta VoIP>.
**Ver detalhes das ROTAS ORIGEM/DESTINO*
ESPAÇO: 1 caractere com espaço em branco para separar a rota de origem do número From de destino.

Destino:

***NÚMERO FROM*:** Até 20 caracteres
Por padrão contém o mesmo número do FROM de origem, salvo quando a saída for via OpVoIP (conforme User da conta selecionada) ou quando este campo for alterado conforme a regra de redirecionamento.

***ESPAÇO*:** 1 caractere com espaço em branco para separar o número From do número To.

NÚMERO TO: Até 20 caracteres.
Contém o número de destino para saída da ligação, manipulado ou não, ou a identificação do usuário de um dos pontos remotos.

***ESPAÇO*:** 1 caractere com espaço em branco para separar o número To da rota de destino.

ROTA DESTINO: 4 caracteres
Identifica a rota de destino: <Interface> + <Grupo Saída, Sip Integrado ou Conta VoIP>.
**Ver detalhes das ROTAS ORIGEM/DESTINO*

ESPAÇO: 1 caractere com espaço em branco para separar a rota de destino e a data

DATA E HORA: 16 caracteres:
Contém a data e hora do bilhete, no formato: “DD/MM/AAAA hh:mm”, onde:
DD – dia do bilhete (dois caracteres)
MM – mês do bilhete (dois caracteres)
AAAA – ano do bilhete (quatro caracteres)

hh – hora do bilhete (dois caracteres)
mm – minutos do bilhete (dois caracteres)

ESPAÇO: 1 caractere com espaço em branco para separar a data da duração

DURAÇÃO: 8 caracteres:
Contém a duração da ligação na forma: "hh:mm:ss", onde:
hh – hora da duração (dois caracteres)
mm – minuto da duração (dois caracteres)
ss – segundos da duração (dois caracteres)

***ROTAS ORIGEM/DESTINO:**
Identifica as rotas de origem e destino através de 4 dígitos <IXNN>, onde:

I (Interface)	**XNN (número de identificação)**
0: Primeiro E1	X: Grupo de Entrada ou Saída [0 a 9] NN: N° do canal E1 [01 a 30]
1: Segundo E1	
2: GSM	sem aplicação
3: Operadora VoIP 1	XNN: N° identificação da conta VoIP [001 a 999]
4: Operadora VoIP 2	
5: Operadora VoIP 3	
6: Operadora VoIP 4	
7: Operadora VoIP 5	
8: Sip Integrado	XNN: N° identificação do Sip Integrado [001 – 064]

Exemplo de bilhetes gerados pela saída de tarifação FTP:

NÚMERO FROM	NÚMERO TO	RO	NÚMERO FROM	NÚMERO TO	RD	DATA INÍCIO	DURAÇÃO
1143063655	200	0002	1143063655	200	8002	08/10/2013 16:21	00:01:10
5185119964	229	0005	5185119964	229	8002	08/10/2013 16:57	00:02:22
244	035911122	8002	5135792200	35911122	0010	06/11/2012 15:10	00:01:00
9	001194565522	8002	5135792200	0151194565522	2102	06/11/2012 15:31	00:03:45
9002	228	8003	9002	228	8002	07/11/2012 08:05	00:01:16
278	091353265	8002	278	91353366	2001	07/11/2012 09:13	00:01:55
5135792200	01121478800	0001	voipaccount	0211121478800	3005	25/09/2013 13:56	00:06:04
5191353345	98214708	2003	5191353345	9	0029	06/10/2013 14:53	00:01:06
5144445555	91353366	0001	5144445555	05191353366	2204	06/10/2013 16:43	00:10:16
5135795000	0215180261384	0001	5135795000	05180261384	2102	06/10/2013 11:04	00:06:04

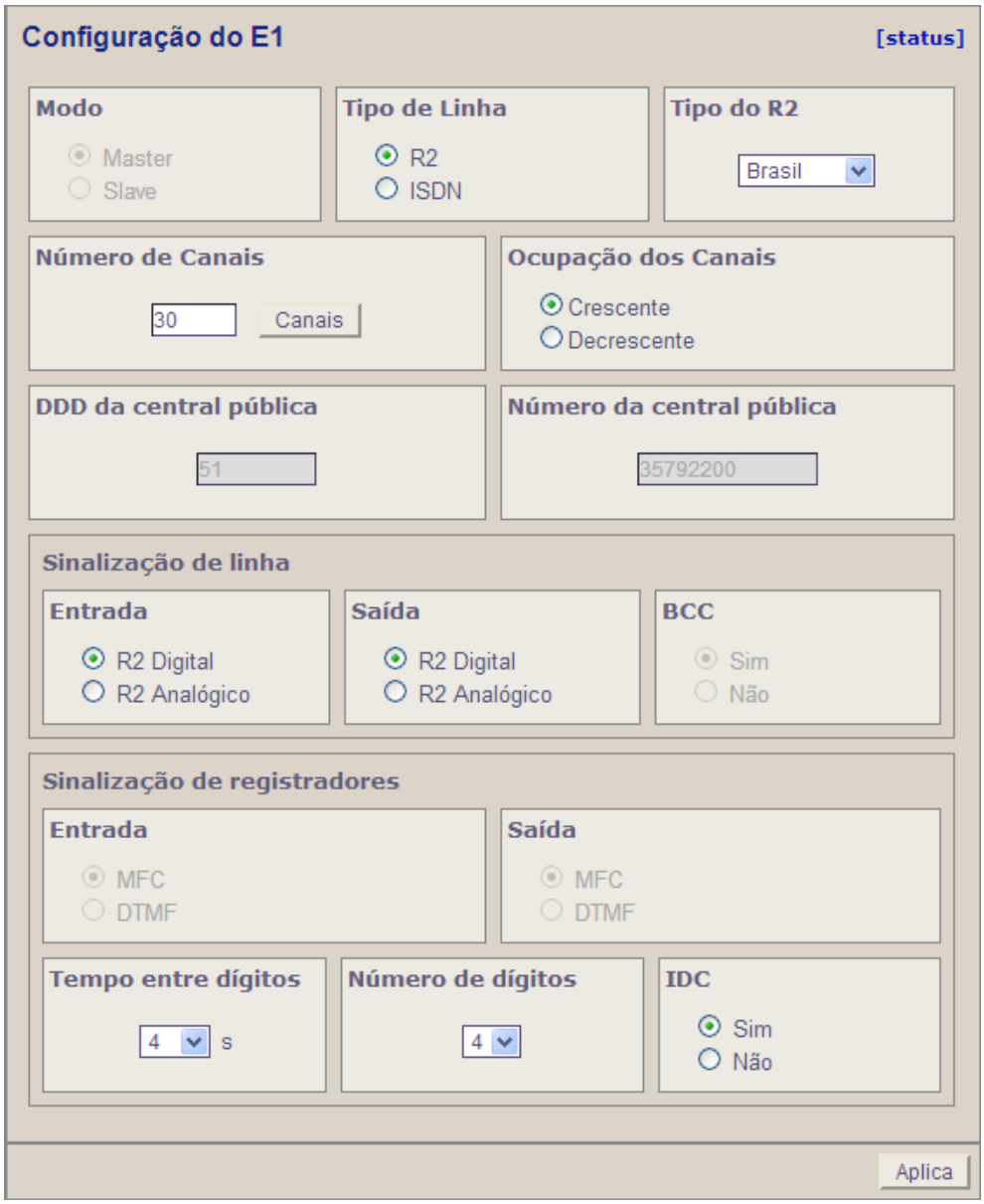
RO: Rota de Origem
RD: Rota de Destino

Exemplo de Rotas de origem e saída:
8001: Rota do Sip Integrado(ponto remoto) 1
8002: Rota do Sip Integrado 2
8003: Rota do Sip Integrado 3
8004: Rota do Sip Integrado 4
0216: Rota primeiro E1, Grupo 2, canal 16 ***(Grupo 2: saída, canais 16 a 30)***
0101: Rota primeiro E1, Grupo 1, canal 1 ***(Grupo 1: entrada, canais 1 a 15)***
0102: Rota primeiro E1, Grupo 1, canal 2
3002: Rota da Operadora VoIP 1, conta 2
4003: Rota da Operadora VoIP 2, conta 3

3.6. TDM

3.6.1. Tronco Digital

A interface E1 necessita ser corretamente configurada, para que a operadora ou PABX e seu Gateway Digistar se comuniquem corretamente.



Modo/Tipo de Linha

Esta é a primeira configuração que deve ser feita para o E1.

São disponibilizados dois protocolos para o enlace E1, o R2 e o ISDN. Os protocolos R2 e ISDN podem operar como Master, onde o gateway opera como uma central pública para ser conectado a um PABX, ou como slave para ser conectado a uma operadora. Apenas um destes deve ser selecionado.

Os campos: Tipo de R2, Sinalização de Linha e Sinalização de Registradores ficam desabilitados ao selecionar a opção ISDN.

Tipo de R2

Devido às diferenças de protocolos utilizados, para o correto funcionamento da sinalização MFC e particularidades do envio de IDC, este campo deve ser selecionado.

Número de canais

Neste campo deve ser configurado o número de canais contratados com a prestadora, sendo assim a configuração do seu E1 é flexível conforme o desejado.

Ocupação dos Canais

Define se a ocupação dos canais do E1 no Gateway Digistar será crescente ou decrescente. Se for configurado como crescente, será escolhido sempre o menor canal E1 disponível para encaminhar ligações para o equipamento conectado à interface E1. Caso for escolhida a opção "decrescente", o gateway selecionará sempre o maior canal disponível. Isso permite diminuir a chance de colisões, uma vez que ao definir uma ordem diferente da utilizada no PABX conectado ao Gateway Digistar, ocorrerá uma colisão somente quando todos os canais forem ocupados.

DDD da Central Pública

Informar neste campo o código DDD do local da instalação.

Sinalização de Linha

Pode ser configurada tanto para entrada como para saída independentemente. A configuração pode ser feita entre R2 analógico (também conhecida como E+M contínua) ou R2 digital. A sua correta configuração deve estar de acordo com sua prestadora.

BCC: Habilita/Desabilita a função de BCC, funcionalidade disponível no E1 modo Slave. Caso o BCC seja habilitado não poderão entrar chamadas a cobrar. Neste caso, se entrar uma chamada a cobrar o Gateway automaticamente derrubará a mesma após o atendimento.

Sinalização de Registradores

Tanto na entrada quanto na saída a sinalização pode ser do tipo MFC (utilizado para comunicação entre centrais públicas) ou do tipo DTMF (utilizada a níveis de assinante), sendo a mesma dos telefones de tom. Na entrada no modo slave e na saída no modo master, são disponibilizados os serviços de DDR e Identificador de chamadas. No modo slave este item deve estar de acordo com a prestadora de serviços telefônicos.

Tempo entre dígitos

Apenas utilizado no modo master. Define o tempo máximo de espera entre os dígitos do número de destino enviados pelo PABX ao Gateway Digistar no protocolo E1 (R2/MFC). Se expirar o tempo máximo para enviar o dígito seguinte, a sequencia digitada pelo executor da chamada será considerada finalizada. Caso esta sequência não for equivalente a nenhuma regra de dígitos da Resolução 86 da Anatel, então o critério de análise para o término da sequência será o tempo desta configuração. Ainda, se o início desta sequência atender a uma regra da Resolução 86, mas não for fornecido o número de dígitos esperados, também a ligação será encaminhada após expirar o tempo entre dígitos.

Número de dígitos

No modo master deve ser definido o número de dígitos recebidos a serem encaminhados. Por exemplo, se forem configurados 4 dígitos e o número de destino recebido na ligação for 3590-3456, os dígitos enviados serão os últimos 4, i.e., 3456. (Obs.: a quantidade de dígitos pode ser menor dependendo das regras definidas na configuração de redirecionamento. Ver seção "Configuração do Redirecionamento de Chamadas"). No modo slave este campo serve para indicar ao gateway quantos dígitos deve requisitar da operadora nas ligações de entrada.

IDC - Identificador de Chamadas

Quando ativado no modo master, o Gateway Digistar irá pedir ao PABX a ele conectado o número de identificação de quem está realizando a chamada (IDC). Para o correto funcionamento, o PABX deve também ser configurado para o envio do IDC. Uma vez recebido pelo Gateway, o IDC será repassado ao destino da ligação. No modo slave o gateway irá enviar o número configurado pela regra de redirecionamento quando solicitado pela operadora.

Envia fim de Discagem (apenas E1 Argentina)

Após o envio do último número de destino por parte do Gateway Digistar, e no caso de que a pública solicite um dígito a mais, deverá ser enviado um sinal MFC "IF" informando o fim da discagem. Este sinal é utilizado para indicação de fim de IDC, mas que aqui será utilizado também para indicar o fim da discagem.

Envia ANI (apenas E1 Argentina)

Envia o ANI para a central pública possibilitando a tarifação por DDR.

Envia IDC (apenas E1 Argentina)

Permite que a central pública envie IDC ao número de destino.

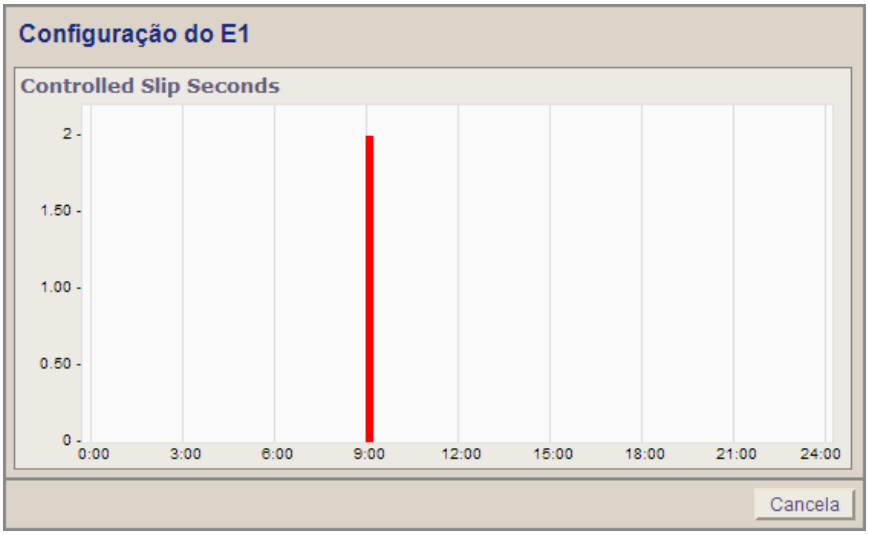
Status

Permite a visualização dos status do link e1. Quando o link estiver sem a presença de alarmes aparecerá "Link Status up". Caso contrário "Link Status down".

Além disso, é possível verificar estatísticas de erros dos últimos 15 minutos e também o histórico das últimas 24 horas. Clicando na opção "more" um gráfico mostrará a ocorrência de erros de 15 em 15 minutos das últimas 24 horas.

As estatísticas estão definidas na RFC 4805 "Definitions of Managed Objects for the DS1, J1, E1, DS2, and E2 Interface Types".

Configuração do E1
Last 15min
Last 24h
Errored Seconds 0 2 more...
Severely Errored Seconds 0 2 more...
Severely Errored Framing Seconds 0 2 more...
Unavailable Seconds 0 0 more...
Controlled Slip Seconds 0 2 more...
Path Coding Violations 0 0 more...
Line Errored Seconds 0 0 more...
Bursty Errored Seconds 0 0 more...
Line Code Violations 0 0 more...
Link Status up
Cancela

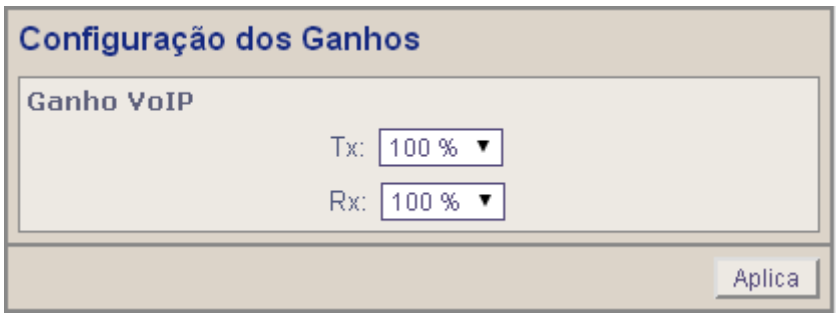


3.6.2. Ganhos

Ganho VoIP: Ganho entre VOIP e uma interface TDM (E1, FXO e GSM)

O nível de áudio na interface VoIP pode ser ajustado em "Sistema→TDM→Ganhos→Ganho VoIP". Podem ser ajustados os níveis de transmissão e recepção.

O nível pode ser ajustado entre 0% e 175%, onde 0% corresponde a "sem áudio", 100% sem ganho ou atenuação e 175% corresponde a um ganho de 75%.

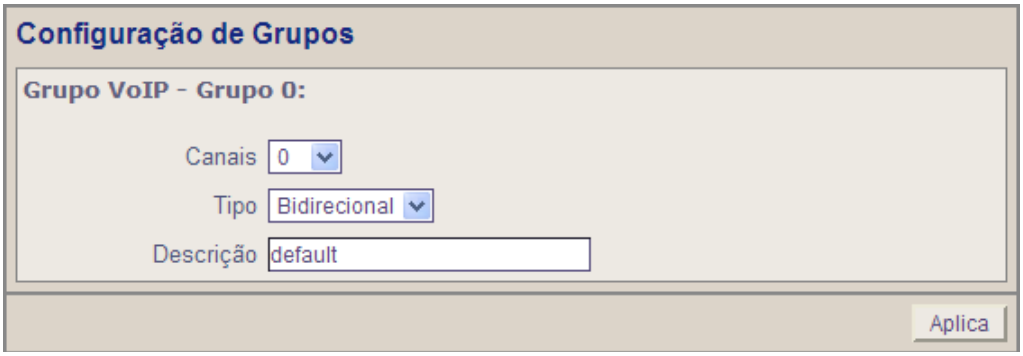


3.6.3. Grupos

Para cada tipo de canal no Gateway Digistar (VoIP ou E1), podem ser configurados até 10 grupos. Estes grupos serão utilizados nas regras de redirecionamento. No caso de grupos E1 e VoIP para cada grupo é definido a quantidade de canais por grupo, ou seja um range de canais para cada grupo.

No campo “Tipo” é possível determinar se os canais do grupo são definidos como somente entrada, somente saída ou bidirecional. Já o campo descrição serve para colocar uma identificação ao usuário sobre a utilidade do grupo para auxiliar na programação das regras de redirecionamento.

Configuração de Grupos
Grupo VoIP
Canais Tipo Descrição
0 60 Bidirecional default
1 0 Bidirecional
2 0 Bidirecional
3 0 Bidirecional
4 0 Bidirecional
5 0 Bidirecional
6 0 Bidirecional
7 0 Bidirecional
8 0 Bidirecional
9 0 Bidirecional
Grupo E1
Canais Tipo Descrição
0 30 Bidirecional default
1 0 Bidirecional
2 0 Bidirecional
3 0 Bidirecional
4 0 Bidirecional
5 0 Bidirecional
6 0 Bidirecional
7 0 Bidirecional
8 0 Bidirecional
9 0 Bidirecional


Configuração de Grupos
Grupo VoIP - Grupo 0:
Canais 0
Tipo Bidirecional
Descrição default
Aplica

3.6.4. Redirecionamento

O correto funcionamento do Gateway Digistar está baseado na programação das regras de redirecionamento de chamadas. A partir da análise das informações das ligações recebidas será feito o tratamento das ligações de saída. De modo a redirecionar as ligações entre as interfaces (TDM e VoIP) é necessário fazer a associação dos números de FROM e TO. Assim, uma ligação recebida ou realizada por um interface utilizará o seu par na outra interface.

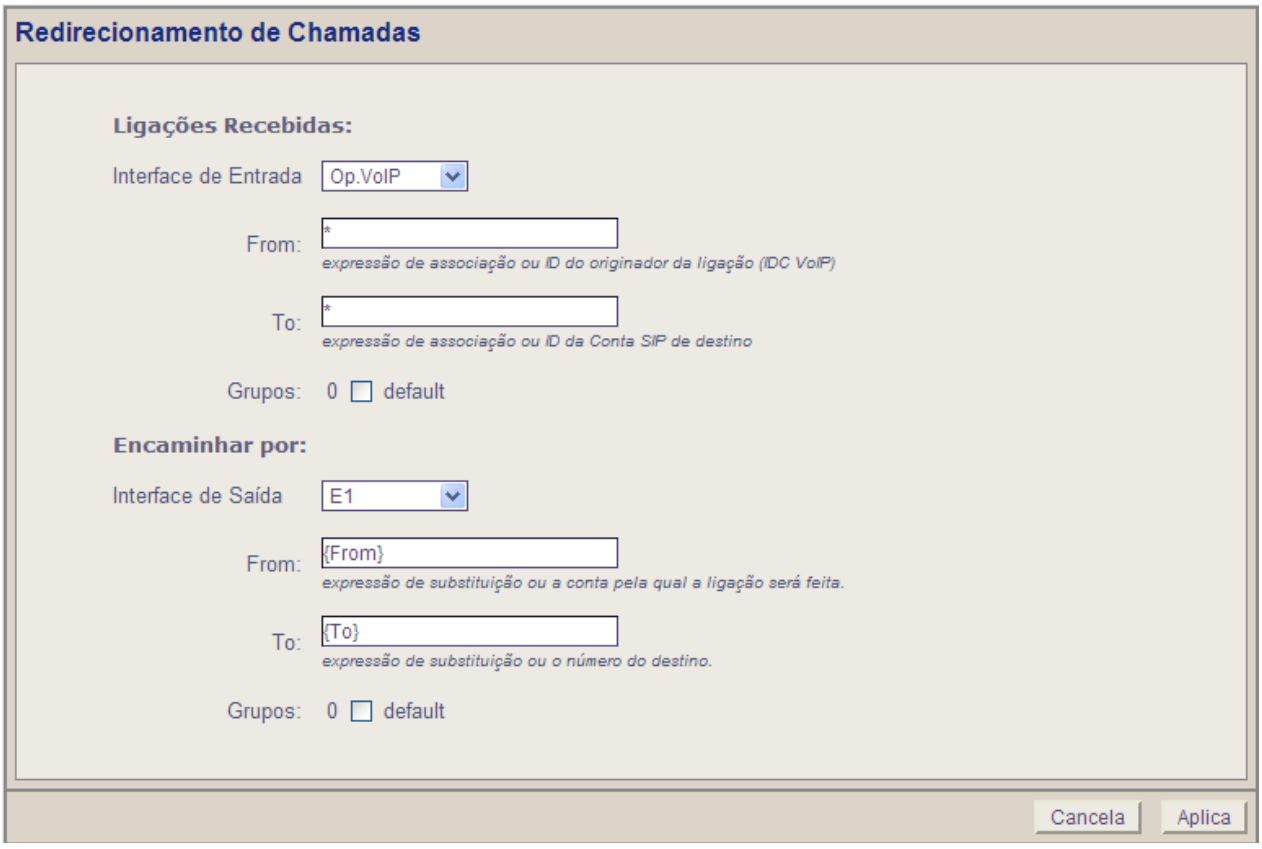
Esses redirecionamentos são configurados utilizando-se de regras com expressões regulares[1], as quais permitem realizar a associação e substituições de modo flexível.

3.6.4.1. Adicionar Regra

Uma nova regra é inserida através do botão “Adicionar nova regra”.

Os botões à direita servem para Alterar, Duplicar ou Remover uma regra existente. O botão “Alterar” edita a regra selecionada abrindo a possibilidade de alterar também a sua prioridade, o botão “Duplicar” cria uma regra idêntica e logo abaixo da regra selecionada, o botão “Remover” remove a regra selecionada.

O gateway Digistar permite alterar a ordem de execução das regras de acordo com a necessidade do usuário, através das setas laterais ou ainda através da opção “Alterar” onde é possível alterar diretamente a prioridade da regra.


Redirecionamento de Chamadas
Ligações Recebidas:
Interface de Entrada Op.VoIP
From: *
expressão de associação ou ID do originador da ligação (IDC VoIP)
To: *
expressão de associação ou ID da Conta SIP de destino
Grupos: 0 default
Encaminhar por:
Interface de Saída E1
From: {From}
expressão de substituição ou a conta pela qual a ligação será feita.
To: {To}
expressão de substituição ou o número do destino.
Grupos: 0 default
Cancela
Aplica

[1] Expressões regulares: provém, por meio de uma linguagem formal, uma maneira concisa e flexível para identificar cadeias de caracteres de interesse, como caracteres específicos, palavras, ou padrões de caracteres.

LIGAÇÕES RECEBIDAS:

Para adicionar uma regra devemos definir as informações da ligação de entrada. Primeiramente a origem. No campo "Interface de entrada" podemos escolher entre os tipos:

- Op. Voip – Operadora VoIP
- Sip Int. – Sip integrado (1 até 64)
- E1 – Entroncamento digital tipo E1 R2 ou ISDN

Definida a interface de entrada é necessário definir o "from" e o "to". Estes campos possuem significados diversos dependendo do tipo de entrada e da posição onde o mesmo foi colocado:

Ex1. Entrada Tipo E1 conectado a uma operadora:

- From = DDD + 8 ou 9 dígitos do número de origem
- To = DDR de 3 ou 4 dígitos

Ex2. Entrada SIP Integrado conectado a um Pabx:

- From – Número de um ramal do PABX remoto
- To – Número da PSTN

Além destes campos, o grupo do canal de entrada da ligação é analisado para auxiliar no encaminhamento da ligação. Com isto é possível fazer reserva de canais para entrada de ligações e encaminhamento dependente da operadora de entrada.

ENCAMINHAR POR :

Após definidas as condições de análise da ligação de entrada, é necessário definir a saída da ligação.

Da mesma forma que na entrada, deverá ser escolhida a interface de saída. Para ligação de saída existe a opção de mais uma interface que é a "DISA". Esta opção direciona a ligação de entrada para uma mensagem gravada. Durante esta mensagem o usuário poderá discar até 20 dígitos. Depois de encerrada a discagem, o Gateway Digistar captura estes números e aplica novamente as regras de redirecionamento. As demais opções de interface de saída são idênticas as da entrada. Não é permitida a interligação entre entrada E1 para saída E1, e entrada Op. VoIP para saída Op.VoIP. É permitido apenas o caso entrada Sip Int. para saída Sip Int.

Já os campos From e To podem ser manipulados para envio ao destino. É possível substituir, incluir ou excluir, parcial ou totalmente, os números recebidos na entrada. Isto se dá através do uso de expressões regulares.

Ex. Uma ligação chega no Gateway Digistar através da Interface de Entrada Sip Int 1 com número de From 266 e To 035792200. Ela deverá ser encaminhada para o E1 com From = 513792 + DDR e sem o "0" no To.

Utilizando expressões regulares devemos configurar:

From = 5135792{From}
To = {To:1}

O Grupo deverá ser escolhido de acordo com o critério desejado pelo usuário. É possível fazer um balanceamento de chamadas reservando canais para um determinado tipo de entrada/saída.

3.6.4.2. Expressões de Associação

As expressões de associação são utilizadas para descreverem as ligações de entrada. Elas são baseadas nas expressões regulares e permitem vincular com uma ou várias ligações. Para isso, pode-se combinar os seguintes comandos:

^	Início da discagem
N	Um dígito: [0-9], [a-z] ou [A-Z]
*	Nenhum ou mais dígitos N
+	Um ou mais dígitos N
?	Nenhum ou um dígito
[x-y]	Intervalos como: [1-3], [a-z]...
[1,4]	Somente dígitos: 1 e 4
$	Fim da discagem
{n,m}	De 'n' a 'm' caracteres
{n}	Exatamente 'n' caracteres

Exemplos:

^NNN Qualquer número de três dígitos (ex.: 201, 356, 999, etc)

^2NN Qualquer número de três dígitos, iniciado com 2 (ex.: 201, 205, 209, etc)

^[0-8] Qualquer número cujo o primeiro dígito esteja entre 0 e 8, isto é, excluindo os que começam com o dígito 9 (ex.:0800, 30303030, 07711.., etc)

* Qualquer número. (ex.: 201, 9090303030, 0800, etc)

3.6.4.3. Expressões de Substituição

As expressões de substituição são utilizadas no encaminhamento das ligações, trocando dígitos ou caracteres para os valores equivalentes na outra interface. A seguir tem-se a sintaxe dessas expressões:

- Expressão de substituição do originador: <num>{From:<offset>:<length>}<num>
- Expressão de substituição de destino: <num>{To:<offset>:< length >} <num>

Com essas expressões é possível referenciar os números originais pelas palavras “From” para o originador e “TO” para o destino. Podem-se acrescentar números antes ou depois (<num>) e também referenciar somente partes dos números originais, possibilitando uma gama de combinações. A referência para parte dos números originais (From ou To) é feita apontando o primeiro digito em <offset> e quantos dígitos, a partir do primeiro, que serão considerados em <length>. Existem algumas considerações:

- O primeiro dígito está na posição zero (offset = 0).
- O offset considera-se da esquerda para a direita.
- Se a length for omitido, então todo o restante dos dígitos, iniciando do offset, será considerado.
- Se offset for omitido e a length for negativo, são considerados os dígitos da direita para a esquerda
- Quando for utilizado offset e length negativo simultaneamente, temos um intervalo, onde length serem desconsiderados da direita para esquerda (atua como um offset no sentido inverso)

Exemplos:

Sendo “To” igual a “30405060”, têm-se os seguintes resultados com as expressões abaixo:

{To:4}	Significado: a partir do dígito na posição quatro, pega todo o resto. Resultado: 5060
{To:0:3}	Significado: a partir do dígito na posição zero, pega três dígitos. Resultado: 304
09988{To}	Significado: acrescenta o prefixo 09988. Resultado: 0998830405060
{To:2:-1}	Significado: pega o intervalo a partir do dígito na posição dois e retira o último algarismo do número. Resultado: 40506

Sendo “From” igual a “2345”, têm-se os seguintes resultados com as expressões abaixo:

{From:-3}	Significado: a partir da direita, pega três dígitos. Resultado: 345
30{From}40	Significado: acrescenta o prefixo 30 e o sufixo 40. Resultado: 30234540

3.6.4.4. Ordem de execução das regras

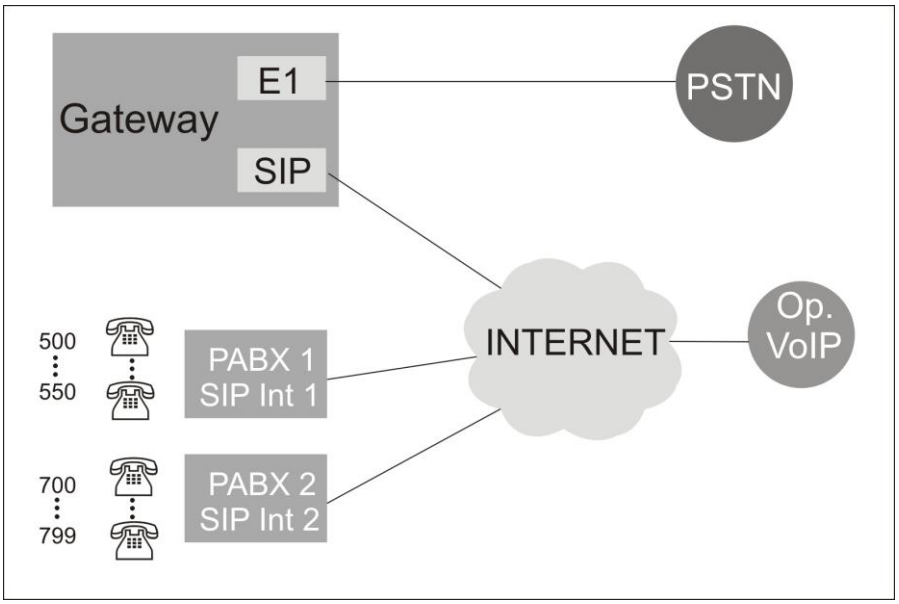
A ordem de execução das regras influência no resultado final. As regras mais prioritárias são as de valor mais baixo, ou seja, a ordem de prioridades é do menor ao maior. As novas regras adicionadas vão para o fim da lista de regras.

3.6.5. Casos de uso

Para fins de exemplo iremos estabelecer sempre o ponto de vista da interface conectada a um usuário ou PABX como origem ou destino. Isto facilita a elaboração dos exemplos de regras de redirecionamento.

3.6.5.1. Caso 1

Usuários conectados através de Sip Integrado. E1 e Op.VoIP conectado a operadoras de telefonia.



No nosso exemplo o Gateway Digistar deverá permitir que os ramais das centrais PABX dos Sip Integrado 1 e 2 da figura deverão poder realizar os seguintes tipos de ligações:

Ligações de Saída a partir do SIP integrado 1:

Regra 0 - Ligações para o DDD 11 deverão ser encaminhadas através do E1 utilizando a operadora de número "21"
Regra 1 - Ligações para os números 35792250 até 35792299 deverão ser encaminhados para os ramais do Sip Integrado 2.
Regra 2 - Ligações DDD para as demais localidades deverão ser encaminhadas para a Op. VoIP 1 na conta "filial1". O número de destino deverá incluir 55+DDD na frente do número para que a operadora VoIP complete a ligação.
Regra 3 - Demais ligações através do E1.

Ligações de Entrada para o Sip Integrado 1:

Regra 4 - Ligações E1 para os DDRs de 200 até 249 deverão ser encaminhadas para os ramais 500 a 549

Ligações de Saída a partir do SIP Integrado 2

Regra 5 - Ligações para o DDD 11 deverão ser encaminhadas através do E1 utilizando a operadora de número "21"
Regra 6 - Ligações DDD para os números 35792200 até 35792249 deverão ser encaminhados para os ramais do Sip Integrado 1.
Regra 7 - Ligações DDD para as demais localidades deverão ser encaminhadas para a Op. VoIP 1 na conta "filial2". O número de destino deverá incluir 55+DDD na frente do número para que a operadora VoIP complete a ligação.
Regra 8 - Demais ligações através do E1

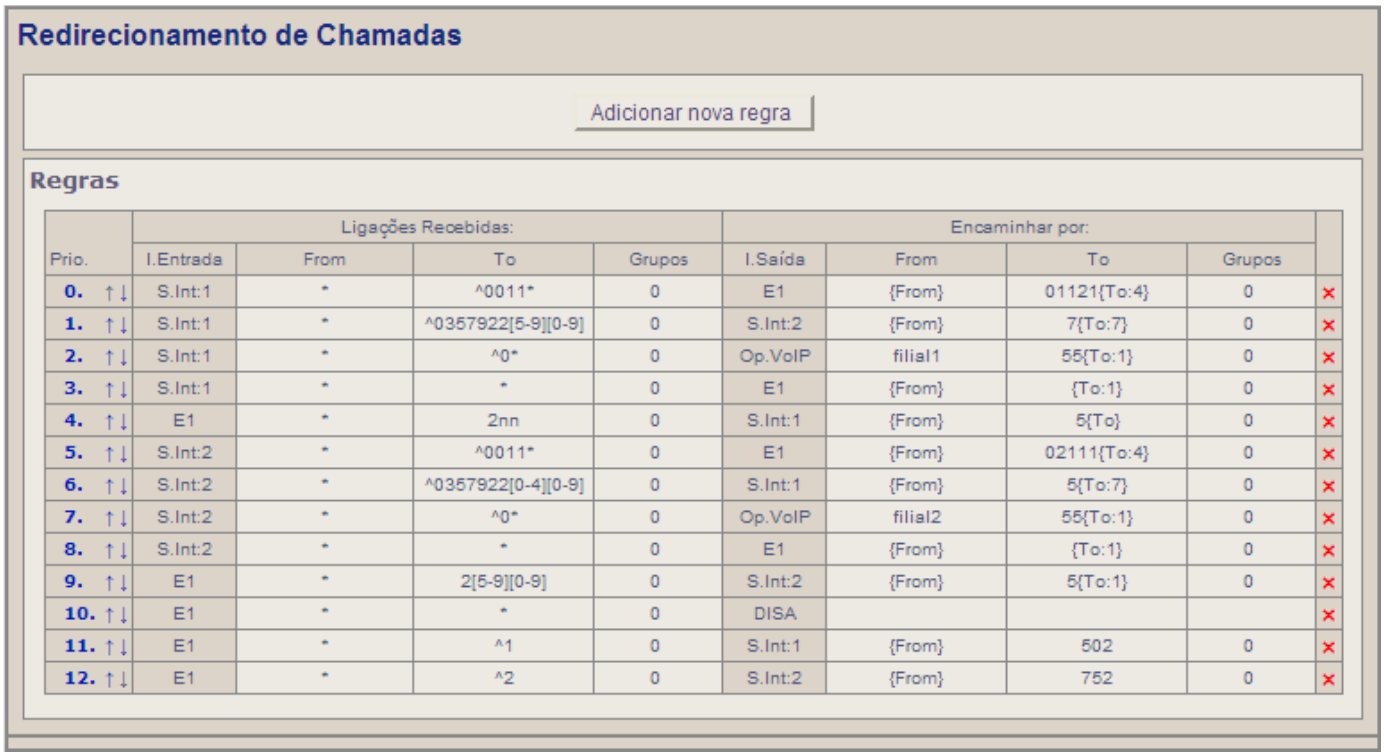
Ligações de Entrada para o Sip Integrado 2:

Regra 9 - Ligações E1 para os DDRs de 250 até 299 deverão ser encaminhadas para os ramais 500 a 549

Ligações DISA:

Regra 10 e 11 – Ligações de entrada através do E1 que não encontrarem correspondência em nenhuma regra anterior deverão ser encaminhadas para o DISA. No DISA caso seja discado apenas o dígito "1" a ligação deverá ser encaminhada para o ramal 502 do Sip Int 1.

Regra 12 – Ligações de entrada através do E1 que não encontrarem correspondência em nenhuma regra anterior deverão ser encaminhadas para o DISA. No DISA caso seja discado apenas o dígito "2" a ligação deverá ser encaminhada para o ramal 702 do Sip Int 2.



Redirecionamento de Chamadas

Adicionar nova regra

Regras

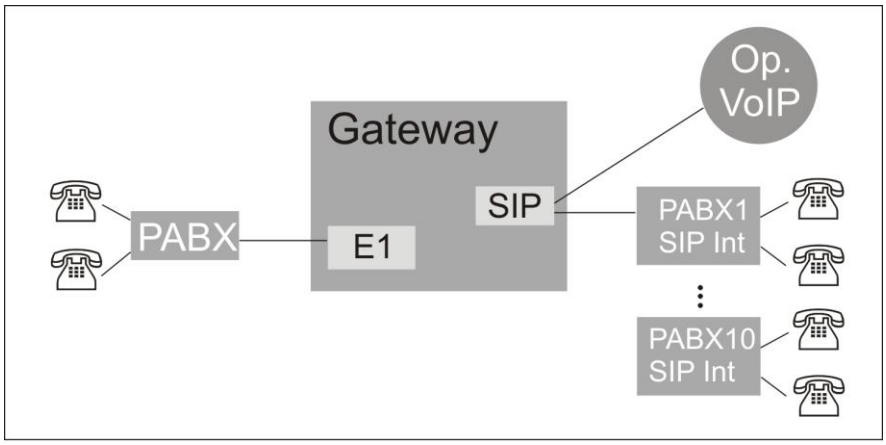
Prio.	Ligações Recebidas:				Encaminhar por:				
	I.Entrada	From	To	Grupos	I.Saída	From	To	Grupos	
0. ↑↓	S.Int:1	*	^0011*	0	E1	{From}	01121{To:4}	0	×
1. ↑↓	S.Int:1	*	^0357922[5-9][0-9]	0	S.Int:2	{From}	7{To:7}	0	×
2. ↑↓	S.Int:1	*	^0*	0	Op.VoIP	filial1	55{To:1}	0	×
3. ↑↓	S.Int:1	*	*	0	E1	{From}	{To:1}	0	×
4. ↑↓	E1	*	2nn	0	S.Int:1	{From}	5{To}	0	×
5. ↑↓	S.Int:2	*	^0011*	0	E1	{From}	02111{To:4}	0	×
6. ↑↓	S.Int:2	*	^0357922[0-4][0-9]	0	S.Int:1	{From}	5{To:7}	0	×
7. ↑↓	S.Int:2	*	^0*	0	Op.VoIP	filial2	55{To:1}	0	×
8. ↑↓	S.Int:2	*	*	0	E1	{From}	{To:1}	0	×
9. ↑↓	E1	*	2[5-9][0-9]	0	S.Int:2	{From}	5{To:1}	0	×
10. ↑↓	E1	*	*	0	DISA				×
11. ↑↓	E1	*	^1	0	S.Int:1	{From}	502	0	×
12. ↑↓	E1	*	^2	0	S.Int:2	{From}	752	0	×

Com isto é possível exemplificar um caso típico de uso onde os PABX 1 e 2 se comunicam entre si através do VoIP, sem custo de ligação, os número fornecidos pela operadora E1 são divulgados para acesso a todos os usuários e os custos de ligação DDD e celular são otimizados através dos usos da Op. VoIP.

Para tanto devemos fazer regras onde o destinatário receba como IDC da ligação o número divulgado para retorno através do E1, ou seja, 1135792 + DDR, independente da interface de saída.

3.6.5.2. Caso 2

Usuários conectados a um PABX legado (sem interface VoIP) através do E1 e Op. VoIP conectadas a operadoras de telefonia.



Ligações de saída através do E1:

Regra 0 – Ligações para os números 35792200 até 35792299 direcionados para os ramais do PABX do sip integrado 1.

Regra 1 - Ligações DDD através do Op Voip 1 inserindo 025+DDD pela conta “matriz”.

Regra 2 – Ligações locais através da Op. VoIP 1 inserindo 02511 pela conta “matriz”.

Ligações de Entrada para o PABX conectado ao E1:

Regra 3 – Ligações recebidas da Op. Voip com to de 30305000 até 30305099 deverão ser encaminhadas os DDRs do E1 no range 500 até 599.

Regra 5 - Ligações recebidas do SIP Integrado 1 com números 1130305000 até 1130305099 deverão ser encaminhadas os DDRs do E1 no range 500 até 599.

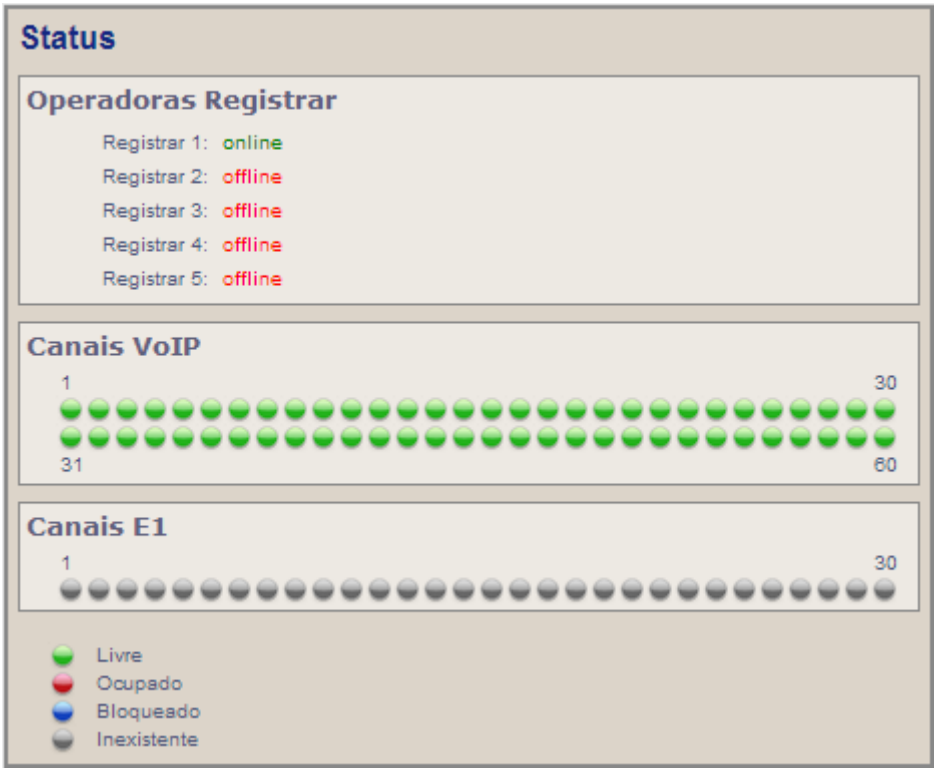
Ligações de Entrada a partir dos Sips Integrados:

Regra 5 - Toda ligação de saída vindas dos SIPs integrados 2,3 e 5 até 9 serão efetuadas através da Op. VoIP pela conta “matriz”.

O caso 2 é um exemplo típico de integração de um PABX legado (sem VoIP) com o mundo IP.

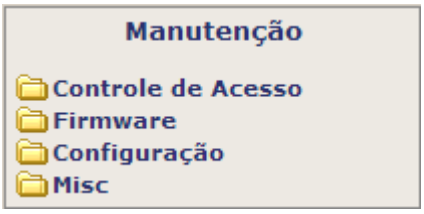
3.6.6. Status

O Gateway Digistar atualiza a cada 10 segundos a tela de status dos canais. Os canais livres estão na cor verde, os ocupados em vermelho, os bloqueados em azul e os inexistentes em cinza. Também é possível verificar por esta o estado das Operadoras Registrar.



4. Manutenção

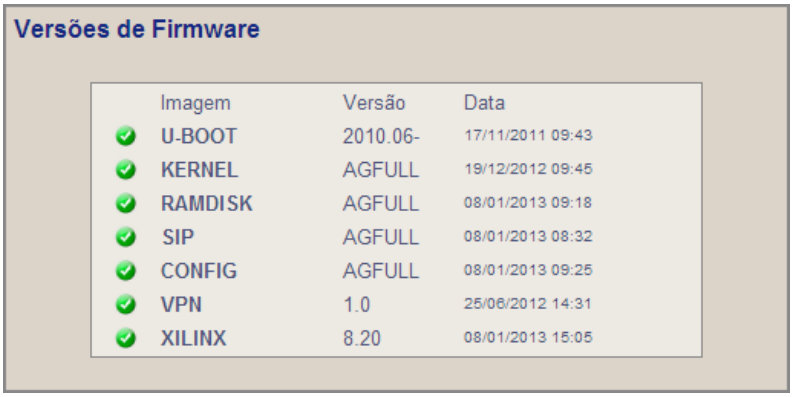
Os itens a seguir são para realizar a manutenção do sistema depois de configurado.



4.1. Firmware

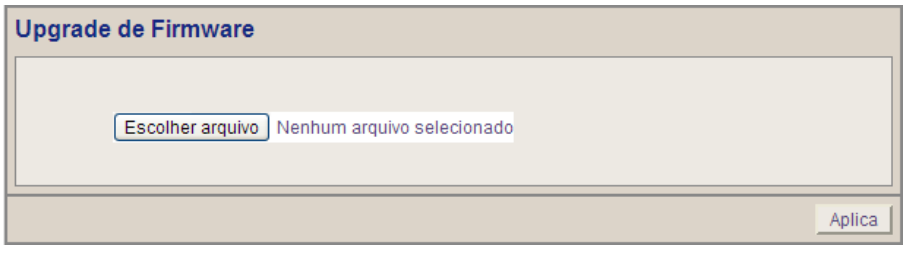
4.1.1. Versões

Tela onde são exibidas as versões de todos os pacotes instalados no Gateway Digistar.



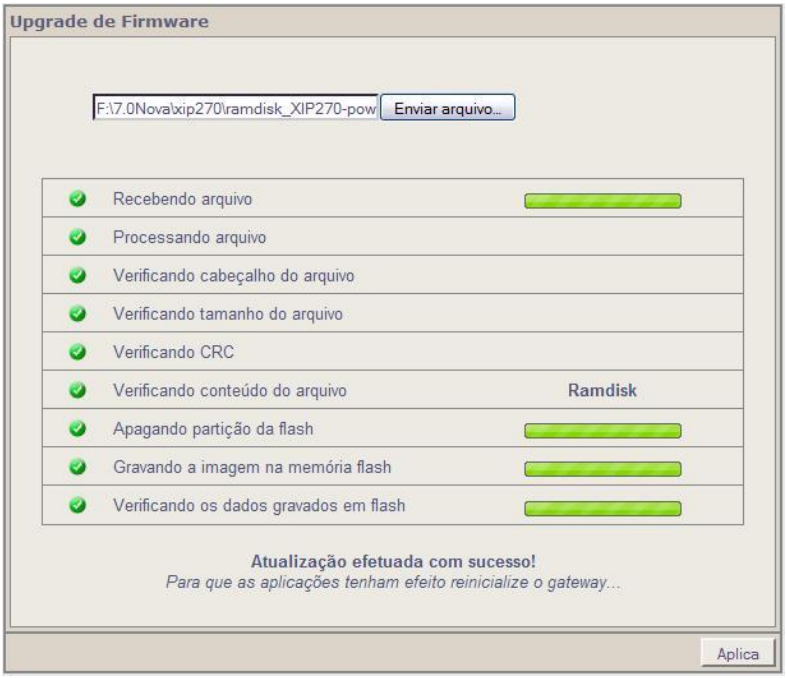
4.1.2. Upgrade de Firmware

Para manter seu Gateway Digistar sempre atualizado existe na opção upgrade de firmware, uma forma bastante simples de operação. Colocando no campo “Upgrade de Firmware”, qualquer pacote de atualização (Kernel, Ramdisk, SIP, Config, VPN ou Xilinx), o Gateway Digistar irá automaticamente identificar o pacote utilizado e efetuar a gravação do novo pacote.



Se a gravação ocorrer com sucesso, você deve reiniciar o Gateway Digistar. Caso haja algum problema, verifique se a imagem não está corrompida, e repita a operação. Para que haja mais segurança a atualização deve ser feita por uma máquina da interface LAN, embora seja possível atualizar pela interface WAN, habilitando o campo respectivo nas configurações gerais do firewall (Ver *"Seção Firewall"*).

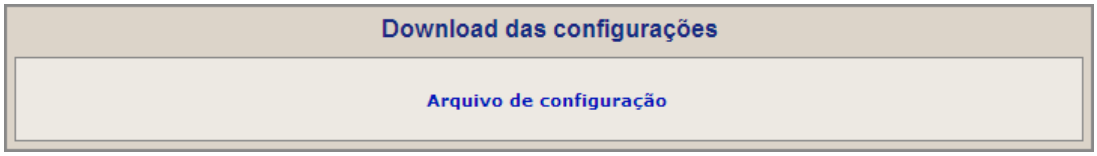
OBS.: *Durante o processo de atualização do firmware alguns serviços podem parar de funcionar. Para o restabelecimento de todas as de todas as funções, aguarde a atualização e resete o Gateway Digistar*



4.2. Configuração

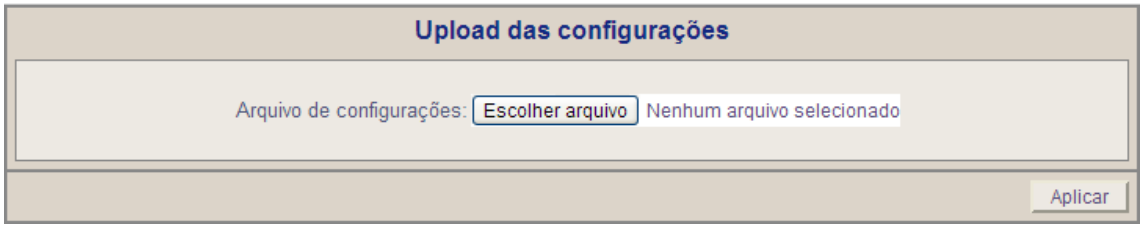
4.2.1. Download

Permite fazer um backup dos arquivos de configuração. Após clicar em download e digitar a senha de programação correta, aparecerá uma tela que permite realizar o download do arquivo de configuração do Gateway Digistar, para um diretório a sua escolha em seu computador.



4.2.2. Upload

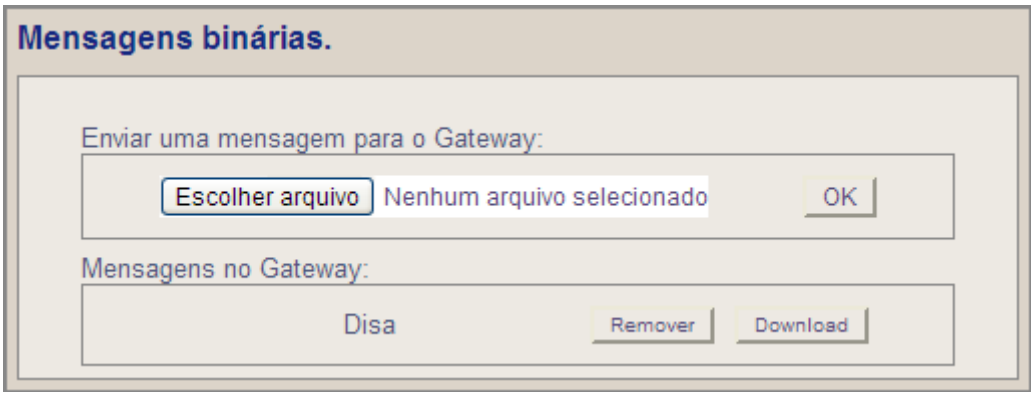
Permite a partir de um backup do arquivo de configuração, voltar a uma configuração feita anteriormente. Após clicar em upload aparecerá uma tela que permite realizar o upload do arquivo de configuração. Procure o diretório do computador, onde está o arquivo baixado anteriormente e clique em "Aplica" para trazer o arquivo do computador para o Gateway Digistar. Para as modificações terem efeito será necessário desligar e ligar o Gateway Digistar.



4.3. Misc

4.3.1. Mensagens Binárias

A mensagem binária DISA é uma mensagem de auxílio ao usuário.



Enviar uma mensagem para o Gateway

Em "Procurar…" escolha o arquivo a ser enviado para ao Gateway Digistar e clique em "OK".

Mensagens no Gateway

Este item exibe todas as mensagens disponíveis no Gateway Digistar. Esta mensagem pode ser removida ou baixada para o PC, clicando no botão apropriado.

4.3.2. Reset Geral

Neste caso as configurações de Gateway Digistar voltarão às configurações de fábrica, ou seja, limpará tudo que fora configurado, inclusive o que está rodando e colocará a configuração de fábrica.

5. Anexo I - Status enviado do SIP para o ISDN no encerramento de ligações.

Status	**Motivo**
case 400	// Bad request
case 401	// Unauthorized
case 402	// Payment required
case 403	// Forbidden
case 404	// Not found
case 405	// Method not allowed
case 406	// Not acceptable
case 407	// Proxy authentication required
case 408	// Request timeout
case 409	// Conflict
case 410	// Gone
case 411	// Length required
case 413	// Request entity too long
case 414	// Request URI (URL) too long
case 415	// Unsupported media type
case 420	// Bad extension
case 480	// Temporarily unavailable
case 481	// Call leg does not exist
case 482	// Loop detected
case 483	// Too many hops
case 484	// Address incomplete
case 485	// Address ambiguous
case 486	// Busy here
case 487	// Request canceled
case 488	// Not acceptable here
case 500	// Internal server error
case 501	// Not implemented
case 502	// Bad gateway
case 503	// Service unavailable
case 504	// Gateway timeout
case 505	// Version not implemented
case 580	// Precondition failed
case 600	// Busy everywhere
case 603	// Decline
case 604	// Does not exist anywhere
case 606	// Not acceptable